Carleton University

Office of the Vice-Provost and Associate Vice-President (Academic)

*memorandum*

DATE: May 30, 2024

TO: Senate

FROM: Dr. David Hornsby, Vice-Provost and Associate Vice-President (Academic), and Chair, Senate Quality Assurance and Planning Committee

RE: Bachelor of Cybersecurity
**New Program Approval**

---

**SQAPC Motion**

THAT SQAPC recommends to Senate the approval of the Bachelor of Cybersecurity program as presented, to commence in Fall 2025.

**Senate Motion**

**THAT** Senate approve the proposed Bachelor of Cybersecurity program as presented to commence in Fall 2025.

**Background**

The School of Computer Science is proposing a new Honours undergraduate degree: the Bachelor of Cybersecurity (B.Cyber). The program is designed to be a national magnet for high-achieving students who are strongly interested in a career in computer and network security. The main educational goal of the program is to prepare students to take on computer and network security-expert roles in government and industry. The program is focusing on a particular segment of the job market for computer and network security specialists and mostly avoids covering "IT-department" work. While the program will expose students to some of the existing technologies, the focus is giving students a deep understanding of the broad range of current and anticipated future threats, risks, and protection against them.

**Attachments**

Self-Study with Appendices (Volume I)
Discussant Report
Site visit Agenda
External Reviewer Biographies
External Reviewers' Report
Unit response to the External Reviewers' Report and Implementation plan
Dean's response to the External Reviewers' Report

SQAPC outcome memo
Dean’s letter of support
Courseleaf Entries
Faculty CVs (Volume II)

**Quality Assurance Framework and Carleton’s Institutional Quality Assurance Process (IQAP)**

Upon the above motion being passed by Senate, the required documentation will be submitted to the Ontario Universities' Council on Quality Assurance for approval. A submission to the Ministry for approval will follow. These approvals are required before the program can commence.

Carleton University

Office of the Provost and Vice-President (Academic)

Institutional Quality Assurance Process

# Bachelor of Cybersecurity (BCyber)

New Program Approval

Volume I

February 2024

# Approvals Table

This table will record that the brief has been approved by: 1) the program lead on behalf of the team; 2) the head of the academic unit or chair of the program committee (in the case of interdisciplinary programs not administered exclusively by one academic unit) on behalf of the unit or program committee; 3) the Faculty Dean(s).

| **Program Lead** | **Date** |
|---|---|

| **Chair/Director** | **Date** |
|---|---|

| **Dean(s):** | **Date** |
|---|---|

**Committee Reviews and Approvals**

| | |
|---|---|
| Vice-Presidents' Academic Research Committee (executive summary) | |
| Provost's Budget Working Group (executive summary) | |
| Curriculum Committee | |
| Faculty Board | |
| Senate Committee on Curriculum, Admissions on Studies Policy | |
| Senate Quality Assurance and Planning Committee | |
| Senate | |
| Quality Council | |

# Table of Contents

# A. The Program

## A.1. Program overview

### A.1.1 Concept

The School of Computer Science (SCS) is proposing a new Honours undergraduate degree: the Bachelor of Cybersecurity (BCyber). The program is designed to be a national magnet for high-achieving students who are strongly interested in a career in security. We believe this is feasible, and attractive to students, for the following reasons.

1. This will be the first program in Canada of its kind.
2. Security courses will be taught by members of one of the country's top research groups in the area, arguably the top amongst groups whose work spans the theory-practice spectrum.
3. There is a recent consensus that in computing-related areas of study, security has emerged as its own distinct area, alongside the other existing top-level areas of Computer Engineering (CE), Computer Science (CS), Information Systems, Information Technology (IT) and Software Engineering (SE).
4. Our experience with the Shopify internship partnership has shown both that it is possible to attract outstanding students to Carleton for a unique program.
5. Ottawa, in addition to having numerous software companies that have a core business interest in security, has, as the nation's capital, the main governmental organizations that have Cybersecurity as a primary focus. These include CSE (Communications Security Establishment), DND and the RCMP. The program's structure will provide for earlier, and more meaningful, co-op opportunities.
6. Since the degree includes most of the core of a standard CS (Computer Science) degree, it will not carry the risk for students of a new kind of degree program that is unknown to employers.
7. The program will have a strong cohort aspect, with limited enrolment and cohort-building components such as exclusive courses and course sections.
8. As has been successfully done with the Shopify internship program, the BCyber will be "front-loaded", using a compressed introduction that will make students employable in co-op positions after their first year.

### A.1.2 Societal need

Our widespread and still rapidly expanding dependence on computers comes with serious risks such as unauthorized access, data manipulation, and exploitation of vulnerabilities that are, despite decades of research, becoming deeper and more widespread because of the increasing complexity of software and software systems. These risks pose a serious threat to our society on many fronts. Our industries, financial infrastructure, government and individuals are at risk of disruption, damage and loss from malicious individuals and groups. The malicious actors can be motivated by financial gain or political/ religious extremism, or they can be part of "cyberwarfare" campaigns of adversarial nation-states. Major news outlets frequently report attacks such as major breaches of individual privacy, and costly payouts and operational recovery due to ransomware.

## A.1.3 Goals

The main educational goal of the program is to prepare students to take on security-expert roles in government and industry. Note that we use the term “security” here to mean “Cybersecurity”. Technically these terms are distinct, but they are similar enough for our purposes to be used synonymously. Also, although privacy is technically a distinct area, here we will include it as part of security.

We are targeting a particular segment of the job market for security specialists. We are not targeting “IT-department” work, which focuses on day-to-day application of existing technologies for securing networks and computers, such as monitoring for intruders on company networks. While our program will need to expose students to some of these technologies, the focus will be giving students a deeper understanding of the broad range of current and anticipated future threats, and defences against them. A typical job for a graduate would be as a security expert on a software development team, or as a member of a unit or organization specializing in computer/internet security.

## A.1.4. Structure

The degree requirements for the BCyber are based on the Bachelor of Computer Science (BCS) honours degree. They include most of a typical BCS core program, plus adaptations of the two basic security courses offered in the BCS Security Stream and 6 new courses on security.

At least two of the advanced courses taken by each student will be project-centred. Projects will typically be related to the research area of the instructor and will give students an opportunity to work on security problems of current societal interest.

Four of the new courses are *Operating Systems Security, Human Factors in Security, Network Security, and Software Security.* The other two security courses are labelled as “Advanced Topics”. The plan is for each offering to focus on a particular area. The areas will vary from offering to offering depending on faculty availability and curriculum needs. See Section B.3 for some details on the Advanced Topics courses.

We are very interested in adapting the Shopify internship model to this program. However, we will leave this to future work since 1) the time needed to set it up could substantially delay the start of the BCyber, and 2) there is substantial employer-recruiting work to be done before we can commit to offering the option. If the option is added, its practicum courses would replace 10 of the free electives of the program.

There are no plans for any non-standard modes of delivery.

## A.1.5. National Profile

We surveyed all the security-related undergraduate options in Canada and found that there are no programs in Canada that have a large part of their curriculum devoted to security, except for one at Ontario Tech (recently renamed from University of Ontario Institute of Technology). There are a number of programs advertising a concentration in the area, and even a major, but, except for Ontario Tech, they all simply collect existing CS courses deemed related to security work and only have a few courses, typically two, and at most four, that focus on security.

The UOIT program has six courses directly in the area, but the courses are squarely within the field of IT (Information Technology), a field that is distinct from CS. CS covers the widest range of computing topics, from theoretical foundations to the development of new computing technologies and techniques. IT focuses on deployment: how to configure, adapt, maintain and operate existing software and software systems, incorporating industry best practices and meeting enterprise needs.

The BCyber, while covering some existing technologies, is focused on producing professionals who understand how to design, build and analyze secure software and systems, and who have sufficient knowledge of the fundamentals to enable them not only to react to changes in the security landscape but to anticipate them.

## A.2. Mission and strategic directions

### Carleton's Strategic Integrated Plan

Carleton's Strategic Integrated Plan (SIP) is organized around three strategic directions.

1. Share the knowledge, shape the future.
2. Serve Ottawa, serve the world.
3. Strive for wellness, strive for sustainability.

The BCyber is an exceptionally strong fit with the first two directions. We are leveraging our research expertise to design and deliver a new curriculum for educating the highly qualified personnel needed to deal with important societal problems. This fits squarely in the first of the two sub-themes of the first direction: preparing students for success in an ever-changing future.

It also fits in the second sub-theme, using our expertise and research to help solve problems important to Canada, since new faculty hires for the BCyber will be doing research in practically important areas of security.

The program will serve Ottawa because of the importance of security to local employers.

1. Software companies are a major part of Ottawa's industrial base. Protection against malicious exploitation, and protection of privacy, are central concerns with most software applications and systems.
2. Ottawa is home to the headquarters of governmental organizations like DND, CSE (which includes the Canadian Cybersecurity Centre) and the RCMP that view cybersecurity as a critically important part of their mission. These employers will benefit from research collaborations with new faculty who are focused on problems of practical significance, and from the much needed access to talent provided by our co-op students and graduates.

## A.3. Relationship to other academic programs at Carleton

The BCyber requires no courses taught by other academic units at Carleton, except for three mathematics/statistics courses already required in all BCS programs, and one mathematics course that will be in a set of security-related electives. The new courses created for the program will be available to all Carleton students meeting the prerequisites, subject to enrolment capacity.

We do not foresee any detrimental enrolment impact on Carleton programs, current or future, in IT or Engineering. Because of accreditation, programs in Engineering do not have room for the degree of specialization in security that is offered by the BCyber. IT programs, as explained earlier, focus on deployment and operation of existing IT products, which is just one small part of the range of security studies in the BCyber.

We do not expect the BCyber to draw significant numbers of students from the existing BCS security stream, or the BCS in general. The specialization and uniqueness of this program will draw new students who would otherwise go to a top Canadian CS university such as Waterloo, University of Toronto or UBC. While it is likely some of the applicants to the BCS security stream would apply to the BCyber, such

students would be competing in a nationally-drawn pool of high-achieving students who have a strong commitment to focusing on security.

We also expect that a few students enrolling in the BCyber at the expense of the BCS will be more than counterbalanced by the increased national visibility of the BCS that the BCyber will provide. This effect has been demonstrated by two of our previous BCS initiatives: the game development stream and Industrial Internship Option partnership with Shopify. Students often decided to come to Carleton for a BCS because we offer attractive content, even if they were not particularly interested in the game or internship programs per se, or they applied to them and were rejected.

# B. Program Learning Outcomes and Assessment

## B.1. Program learning outcomes and degree level expectations

The following are the learning outcomes for the BCyber. Each one is given a convenient name for reference.

**Context.** Be able to explain how security principles and mechanisms relate to the current computing and communication infrastructure and ecosystems.

**Dev.** Be able to design and implement programs to solve problems in a range of application domains, applying established software engineering concepts, techniques and environments, with special attention to software and systems security.

**Cryptography.** Be able to apply cryptography-based methods in software development, with an understanding of the impact on both systems/communications security and on end users.

**Attacks.** Be able to apply knowledge of the wide range of possible methods for attacking software and computing systems, and of common software vulnerabilities that enable them, in software development and in the critique of existing systems from a security perspective.

**Analysis.** Be able to analyze and test software and networked systems for security flaws and risks, and be familiar with exemplars of relevant state-of-the-art tools and mechanisms.

**Stack.** Be able to apply an understanding of the layers of abstraction between modern networked software systems and the underlying computer hardware (the "computing stack") in analyzing systems for security flaws and in the development of secure software.

**Languages.** Be able to explain the principle concepts of programming languages, especially security relevant aspects, and be proficient at developing software systems and programs in at least one systems language and one higher-level language.

**Advanced.** Develop knowledge in at least one specialized, state-of-the-art security topic.

**Independence.** Conduct independent work to create a major security-related software artifact or a contribution to security research.

## B.2. Mapping learning outcomes to provincial DLEs

The Council of Ontario Universities has established a framework of Degree Level Expectations (DLEs) that specify what students should know, and be able to do, after successfully completing a degree program. They are:

1. Depth and breadth of knowledge
2. Knowledge of methodologies
3. Application of knowledge
4. Communication skills
5. Awareness of the limits of knowledge
6. Autonomy and professional capacity
7. Experiential Learning

Table B.2 maps each BCyber learning outcome to the DLEs it contributes to.

Table B.2: Learning outcomes and degree level expectations

| **Learning Outcomes** | **Degree Level Expectations Met** | **Notes** |
|---|---|---|
| **Context**<br>Be able to explain how security principles and mechanisms relate to the current computing and communication infrastructure and ecosystems. | 1. Depth and breadth of knowledge<br>4. Communication skills<br>5. Awareness of the limits of knowledge<br>6. Autonomy and professional capacity | The LO focuses on societal context, which is a form of breadth, hence DLE 1. DLE 2 follows from the "explain" part of the LO. Relating security to context inherently involves discussion of limits and the role of security professionals, hence DLEs 5 and 6. |
| **Dev**<br>Be able to design and implement programs to solve problems in a range application domains, applying established software engineering concepts, techniques and environments, and with special attention to software and systems security. | 2. Knowledge of methodologies<br>3. Application of knowledge<br>4. Communication skills<br>7. Experiential Learning | DLEs 2 and 3 are central parts of software development. The **Dev** LO contributes to communication skills since development requires clear documentation. The numerous courses contributing to **Dev** are heavily oriented toward "learning by doing" and use actual software development as the main kind of student term work. |
| **Cryptography**<br>Be able to apply cryptography-based methods in software development, with an understanding of the impact on both systems/communications security and on end users. | 2. Knowledge of methodologies<br>3. Application of knowledge<br>5. Awareness of the limits of knowledge<br>7. Experiential Learning | Experiential learning is implicit in the application to software development, as outlined above. Understanding the impact of cryptography involves understanding the limits of cryptography's security guarantees. |

| | | |
|---|---|---|
| **Attacks**<br>Be able to apply knowledge of the wide range of possible methods for attacking software and computing systems, and of common software vulnerabilities that enable them, in software development, and in the critique of existing systems from a security perspective. | 1. Depth and breadth of knowledge<br>2. Knowledge of methodologies<br>5. Awareness of the limits of knowledge | The "wide range" referred to involves a huge variety of software/systems and the ways they are deployed, hence the breadth part of DLE1. The focus of the LO is methodologies for attacks and for finding vulnerabilities to attack, hence DLE 2. The LO requires understanding the limits of current techniques for securing software and systems, hence DLE 5. |
| **Analysis**<br>Be able to analyse and test software and networked systems for security flaws and risks, and be familiar with exemplars of relevant state-of-the-art tools and mechanisms. | 2. Knowledge of methodologies<br>3. Application of knowledge<br>5. Awareness of the limits of knowledge | The subject of software testing is mainly about methodologies. |
| **Stack**<br>Be able to apply an understanding of the layers of abstraction between modern networked software systems and the underlying computer hardware (the "computing stack") in analyzing systems for security flaws and in the development of secure software. | 1. Depth and breadth of knowledge<br>7. Experiential Learning | Experiential learning is part of the software development outcome. |
| **Languages**<br>Be able to explain the principle concepts of programming languages, especially security relevant aspects, and be proficient at developing software systems and programs in at least one systems language and one higher-level language. | 1. Depth and breadth of knowledge<br>2. Knowledge of methodologies<br>3. Application of knowledge<br>4. Communication skills<br>7. Experiential Learning | Reasons for DLEs 2 to 7 are similar to **Dev**. DLE 1 is because "concepts of programming languages" implies a comparative understanding of the wide range of features found in modern languages. |
| **Advanced**<br>Develop knowledge in at least one specialised, state-of-the-art security topic. | 1. Depth and breadth of knowledge<br>4. Communication skills<br>6. Autonomy and professional capacity | While 4 and 6 do not follow directly from the LO, it will be a central part of the courses establishing it. The courses will be based on team projects that have a strong "real world" component and require both presentation and documentation. |

| | | |
|---|---|---|
| **Independence**<br>Conduct independent work to create a major security-related software artifact or a contribution to security research. | 1. Depth and breadth of knowledge<br>3. Application of knowledge<br>4. Communication skills<br>6. Autonomy and professional capacity | This LO obviously contributes to the depth part of DLE 1 and to DLEs 3 and 6. It requires documentation/presentation of the independent work done, hence DLE 5. |

## B.3. Program structure and curriculum map

### Program structure

The degree requirements for the BCyber are based on the Bachelor of Computer Science (BCS) honours degree. All the BCS Computer Science and Mathematics/Statistics required courses of the BCS are also required in the BCS with the following four exceptions.

1. COMP 3005 Database Management Systems
2. COMP 3007 Programming Paradigms
3. COMP 3804 Design and Analysis of Algorithms I
4. One mathematics or statistics course at the 2000 level above.

The complete set of requirements can be summarized as follows. See Appendix 1 for the calendar copy for the program, and Appendix 2 for courses.

1. 13 existing courses from the BCS core program: 10 in CS, and 3 in mathematics/statistics.
2. 3 existing BCS courses not in the core: HCI, networks, and an introductory second-year security/ privacy course designed for the BCS.
3. 2 introductory courses in security that are based on existing BCS courses but adapted for the needs of the BCyber.
4. 6 new advanced courses in security.
5. 2 electives from a list of 5 related courses in CS and mathematics/statistics.
6. 14 free electives.

At least two of the new advanced courses taken by each student must be project-centred. Projects will typically be related to the research area of the instructor and will give students an opportunity to work on security problems of current research interest. The set of courses that have projects may vary from year to year. The program's curriculum committee will ensure that students all have a sufficient set of project courses to choose from.

The required six advanced courses in security comprise four courses with specified areas and two "advanced topics" courses whose content will vary from year to year, partly to keep up with the rapid pace of change in the theory and practice of security.

The calendar descriptions of the four courses with specified areas are as follows.

*Operating Systems Security.* The course examines past, present, and emerging approaches for securing operating systems. The focus is to provide a foundation for understanding requirements for securing hosts at the operating system level, and to survey the landscape of available tools and techniques for implementing operating system security controls.

*Human Factors in Security.* Designing security mechanisms with human factors in mind. Evaluating software-based systems with focus on how interaction design affects security and privacy. Current approaches to usable security; user studies; methodologies for empirical analysis; design principles for usable security and privacy; case studies including authentication, anonymity systems.

*Network Security.* Security throughout network stack layers. Internet core security. VPNs and tunnelling protocols. Firewalls and Intrusion Detection Systems. Internet measurements. IoT security. Botnets. Securing network protocols, including email and web. Network monitoring. Traffic sniffers and vulnerability scanners.

*Software Security.* Resilience of everyday software to vulnerabilities. Security engineering and the security development lifecycle. Static analysis and vulnerability analysis. Model checkers. Security testing, non-functional testing, fuzz-testing. Programming languages and security. Cryptographic APIs and use of security toolkits.

As the two "advanced topics" courses will not be needed for several years, we do not fix any particular subjects for them at this point. If the courses were being offered next year, they would be among the following.

- Trusted Execution Environments.
- Advanced Authentication and Authorization.
- Cloud Security and Virtualization.
- Web and Browser Security.
- Privacy on the Internet.
- Cryptocurrencies and Blockchain Applications.
- Computer Forensics.

## Program curriculum map

We map the learning outcomes to the set of courses that collectively meet them. We use the following tags on courses to indicate the level at which the course is delivered relative to the learning outcome the course is being associated with.

I: Introductory
R: Reinforcement
M: Mastery

We do not include any specification of "Activities and Artifacts" in the curriculum map. Typically these will be assignments with problems to be solved. Courses may also have larger projects, usually involving some kind of software development or analysis. The choice of how best to meet the requisite learning outcomes will be left to the instructor, though the curriculum committee for the program will need to ensure that a sufficient number of advanced courses be project-based (see above).

The mapping is in Table B.3.

Table B.3 Curriculum Map

| Learning Outcome | Level | Course |
|---|---|---|
| Context | I | COMP 2401 Introduction to Systems Programming |
| Context | I | COMP 2404 Introduction to Software Engineering |
| Context | I | COMP 2406 Fundamentals of Web Applications |
| Context | I | COMP 3004 Object-Oriented Software Engineering |
| Context | I | COMP 2109 Introduction to Security and Privacy |
| Context | I | COMP 3008 Human-Computer Interaction |
| Context | R | CYB 3108 Computer Systems Security |
| Context | R | COMP 4203 Wireless Networks and Security |
| Context | R | CYB 4000 Operating Systems Security |
| Context | M | CYB 4100 Human Factors in Security |
| Context | M | CYB 4200 Network Security |
| Dev | I | COMP 1405 Introduction to Computer Science I |
| Dev | I | COMP 1406 Introduction to Computer Science II |
| Dev | R | COMP 2401 Introduction to Systems Programming |
| Dev | R | COMP 2402 Abstract Data Types and Algorithms |
| Dev | R | COMP 2404 Introduction to Software Engineering |
| Dev | R | COMP 2406 Fundamentals of Web Applications |
| Dev | R | COMP 3000 Operating Systems |
| Dev | R | COMP 3008 Human-Computer Interaction |
| Dev | R | CYB 3108 Computer Systems Security |
| Dev | R | COMP 3002 Compiler Construction |
| Dev | M | COMP 3004 Object-Oriented Software Engineering |
| Dev | M | COMP 4004 Software Quality Assurance |
| Dev | M | CYB 4100 Computer Security and Usabilit |
| Cryptography | I | COMP 1805 Discrete Structures I |
| Cryptography | I | COMP 2804 Discrete Structures II |
| Cryptography | R | CYB 3108 Computer Systems Security |
| Cryptography | R | CYB 4000 Operating Systems Security |
| Cryptography | R | CYB 4100 Human Factors in Security |

| | | |
|---|---|---|
| Cryptography | R | CYB 4200 Network Security |
| Cryptography | R | CYB 4300 Software Security |
| Cryptography | M | CYB 2108 Applied Cryptography and Authentication |
| Attacks | I | CYB 2108 Applied Cryptography and Authentication |
| Attacks | I | COMP 2109 Introduction to Security and Privacy |
| Attacks | I | COMP 2404 Introduction to Software Engineering |
| Attacks | I | COMP 2406 Fundamentals of Web Applications |
| Attacks | I | COMP 3004 Object-Oriented Software Engineering |
| Attacks | I | CYB 3108 Computer Systems Security |
| Attacks | R | COMP 3008 Human-Computer Interaction |
| Attacks | R | COMP 3203 Principles of Computer Networks |
| Attacks | R | COMP 4203 Wireless Networks and Security |
| Attacks | M | CYB 4000 Operating Systems Security |
| Attacks | M | CYB 4100 Human Factors in Security |
| Attacks | M | CYB 4200 Network Security |
| Attacks | M | CYB 4300 Software Security |
| Analysis | I | COMP 2404 Introduction to Software Engineering |
| Analysis | I | COMP 2406 Fundamentals of Web Applications |
| Analysis | I | COMP 3000 Operating Systems |
| Analysis | I | COMP 3004 Object-Oriented Software Engineerin |
| Analysis | I | COMP 2109 Introduction to Security and Privacy |
| Analysis | I | COMP 3008 Human-Computer Interaction |
| Analysis | I | CYB 3108 Computer Systems Security |
| Analysis | I | COMP 4004 Software Quality Assurance |
| Analysis | I | COMP 4203 Wireless Networks and Securit |
| Analysis | M | CYB 4000 Operating Systems Security |
| Analysis | M | CYB 4100 Human Factors in Security |
| Analysis | M | CYB 4200 Network Security |
| Analysis | M | CYB 4300 Software Security |
| Stack | I | COMP 2401 Introduction to Systems Programming |
| Stack | I | COMP 2406 Fundamentals of Web Applications |

| | | |
|---|---|---|
| Stack | I | COMP 3000 Operating Systems |
| Stack | I | COMP 3203 Principles of Computer Networks |
| Stack | I | COMP 3002 Compiler Construction |
| Stack | R | CYB 3108 Computer Systems Security |
| Stack | M | CYB 4000 Operating Systems Security |
| Stack | M | CYB 4200 Network Security |
| Languages | I | COMP 1405 Introduction to Computer Science I |
| Languages | I | COMP 1406 Introduction to Computer Science II |
| Languages | I | COMP 2401 Introduction to Systems Programming |
| Languages | I | COMP 2402 Abstract Data Types and Algorithms |
| Languages | R | COMP 2404 Introduction to Software Engineering |
| Languages | R | COMP 2406 Fundamentals of Web Applications |
| Languages | R | COMP 3000 Operating Systems |
| Languages | R | COMP 3004 Object-Oriented Software Engineering |
| Languages | R | COMP 3002 Compiler Constructio |
| Advanced | M | CYB 4000 Operating Systems Security |
| Advanced | M | CYB 4100 Human Factors in Security |
| Advanced | M | CYB 4200 Network Security |
| Advanced | M | CYB 4300 Software Security |
| Advanced | M | CYB 4900 Advanced Topics in Security I |
| Advanced | M | CYB 4900 Advanced Topics in Security I |
| Independence | M | CYB 4000 Operating Systems Security |
| Independence | M | CYB 4100 Human Factors in Security |
| Independence | M | CYB 4200 Network Security |
| Independence | M | CYB 4300 Software Security |
| Independence | M | CYB 4900 Advanced Topics in Security I |
| Independence | M | CYB 4900 Advanced Topics in Security II |

## B.4. Program learning outcomes assessment plan

We outline an assessment plan to identify the degree to which the BCyber programs are meeting their educational goals, as specified in the learning outcomes.

The assessment of the learning outcomes will be conducted by the curriculum committee (see section C on governance).

The main sources of evidence that will be used to conduct the assessment are a course outline repository, a course material repository and a database of marks obtained by the students. At the beginning of every term, the outlines of all courses offered by SCS are uploaded in the course outline repository. At the end of every term, course material, including lecture notes, slides, assignments, exercises, quizzes, tests and exams, are uploaded in the course material repository, along with low/average/high scoring exemplars of student work. For the advanced security courses that are project-based, all student projects will be included. The curriculum committee members have access to both repositories.

Because the program has many new security-specific courses with no established models, it is important for us to get early feedback. We plan to assess all learning outcomes in the third year, even though many of the courses contributing to them will not have been offered yet. The second assessments of each LO will be done as follows.

Year 5: *Dev, Stack, Languages*
Year 6: *Attacks, Cryptography, Analysis, Context*
Year 7: *Advanced, Independence*

SCS has a School Council consisting of all faculty members appointed to the School (excluding status-only cross-appointments), the School Administrator, and several student representatives. There are four regular meetings per year. The results of the assessment will be distributed, presented and reviewed during school councils.

The curriculum committee will oversee handling of recommendations resulting from the assessment plan. The action plan could include: revision of School-internal guidelines to instructors, adjustment of prerequisites, or revisions to course content.

## B.5. Program essential requirements

Program essential requirements are defined by the Ontario Human Rights Commission as “the knowledge and skills that must be acquired or demonstrated in order for a student to successfully meet the learning objectives of that… program.” The program essential requirements are components that contribute to the achievement of the learning outcomes of the program.

Appropriate accommodations should not lead to lowered standards or outcomes: rather, an appropriate accommodation will enable the student to successfully meet the essential requirements of the program, with no alteration in standards or outcomes, although the manner in which the student demonstrates mastery, knowledge and skills may be altered.

The aim of accommodation in a post-secondary educational context is to provide equal opportunities to all students to enjoy the same level of benefits and privileges and meet the requirements for acquiring an education. Based on these principles, an accommodation will be considered appropriate where it will result in equal opportunity to attain the same level of performance, or enjoy the same level of benefits and privileges experienced by others, or if it is proposed or adopted for the purpose of achieving equal opportunity and meets the individual’s disability-related needs. - See more at: http://www.ohrc.on.ca/en/opportunity-succeed-achieving-barrier-free-education-students-disabilities.

### Paul Menton Centre

The Paul Menton Centre is responsible for assessing requests for academic accommodation of students with disabilities through evaluations that are carried out on an individual basis, in accordance with

human rights legislation and University policy, and with the support of relevant, professional/medical documentation. Students will only receive academic accommodation if the functional limitations of their disability impact directly on their academic performance.

The program essential requirements of the Bachelor of Cybersecurity program have been reviewed in consultation with the Paul Menton Centre to ensure capacity for reasonable academic accommodation of students with disabilities, in accordance with the Carleton University Academic Accommodation Policy. The learning outcomes can be attained as outlined in the program description with the use of appropriate academic accommodations.

# C. Governance

The School currently has eleven faculty with expertise in security. Six more will be added as the program ramps up. This is sufficient for staffing the required governance committees without unusual administrative burden for faculty.

The planned governance structure is as follows. All the new roles/membership mentioned below are restricted to core faculty (see section D for a listing).

## Core faculty

The core faculty of the program are the SCS faculty who have security as a main research area or bring to the program substantial related teaching expertise. As the program progresses additions to the core faculty will be made by the program Director (see below) in consultation with rest of the existing core faculty and the SCS Director.

## BCyber Director

The Director of the program will be appointed for a three-year term by the Director of the School of Computer Science in consultation with the program's core faculty. Teaching relief of one course will be given. The Director will advise the SCS Director on the membership of program committees. All appointments to committees will be made by the SCS Director as part of the School's assignment of administrative tasks. The BCyber Director will be the main faculty resource for the SCS undergraduate advising staff and will work with the SCS School Administrator on program day-to-day operational details.

## Curriculum committee

The committee will formulate and evaluate proposals for BCyber calendar changes. Any formal calendar change submissions will go through the School's usual approval process for BCS changes. The committee will work closely with the SCS curriculum committee and the BCyber Director to ensure that proposed changes are assessed for impact on the offerings and resources of SCS.

## Admissions committee

The admissions committee will make the final decision on admission for all candidates that meet the calendar requirements for admission, subject to general enrolment management requirements of Carleton Admissions and the School of Computer Science.

## Program Assessment Committee(s)

As the assessment of learning outcomes will directly use the assessment from the BCS for the large number of non-security computer science courses, the committee will only be assessing LOs, or parts of LOs, that are specific to security.

# D. The Faculty

## D.1. Faculty appointed to the unit or program

Table D.1 lists the tentative core faculty of the program. These are the SCS faculty who have security as a main research area or bring to the program substantial related teaching expertise. They all have a 100% FTE appointment to SCS.

Table D.1 Core Faculty of the Program

| **Name** | **Rank** | **Status** | **Specialization** |
|---|---|---|---|
| Abdou | Assistant Professor | Preliminary | Internet Security |
| Barrera | Assistant Professor | Preliminary | Computer and Network Security, Internet of Things Security, Operating Systems Security |
| Barbeau | Professor | Tenured | Ad hoc networks, underwater networks, quantum communications and networks, software-defined radio. |
| Biddle | Professor | Tenured | Human Computer Interaction, Computer Security, Computer Games, Agile Software Development |
| Chiasson | Professor | Tenured | Usable security, Human-Computer Interaction, Computer Security, Educational games |
| Hinek | Instructor III | Tenured | Computer Science Education, Cryptology, Security |
| Laurendeau | Instructor III | Tenured | Software engineering, wireless network security |
| Somayaji | Associate Professor | Tenured | Computer Security, Operating Systems, Intrusion Detection, Complex Adaptive Systems, Artificial Life |
| Stobert | Assistant Professor | Preliminary | Human-Computer Interaction and Computer Security |
| Van Oorschot | Professor | Tenured | Authentication, Computer Security, Internet Security, Applied Cryptography, Information Security |
| Zhao | Assistant Professor | Preliminary | Trusted computing, Hardware/architectural security support, Systems security, Authentication and privacy |

The BCyber has a total of nine courses focusing on security. The core faculty will be responsible for teaching eight of them. Table D.2 is a table giving the courses, their level (1000-4000 for first-fourth year), and core faculty with expertise in the course subject.

Table D.2 Security Courses and Core Faculty Expertise

| **Course** | **Level** | **Faculty having the required expertise** |
|---|---|---|
| CYB 2108: Applied Cryptography and Authentication | 2000 | Barrera, Hinek, Van Oorschot |
| COMP 2109: Introduction to Security and Privacy | 2000 | Any core faculty member |
| CYB 3108: Computer Systems Security | 4000 | Abdou, Barrera, Somayaji, Van Oorschot, Zhao |
| CYB 4000: Operating Systems Security | 4000 | Barrera, Somayaji, Zhao |
| CYB 4100: Human Factors in Security | 4000 | Biddle, Chiasson, Stobert |
| CYB 4200 Network Security | 4000 | Abdou, Barrera, Somayaji, Van Oorschot |
| CYB 4300: Software Security | 4000 | Abdou, Barrera, Van Oorschot |
| CYB 4900: Selected Topics in Security I | 4000 | Course content will vary depending on available expertise |
| CYB 4901: Selected Topics in Security II | 4000 | Course content will vary depending on available expertise |

Following are some comments related to the core faculty and the delivery of the new program.

- *Teaching load.* The standard teaching load in SCS is one graduate course and two undergraduate courses. While two of the faculty currently hold research awards supplying some teaching relief, these will have expired by the time the program starts. Apart from sabbaticals and new teaching relief (e.g. for BCyber governance), all the research-stream core faculty will teach two undergraduate courses per academic year.
- *Missing expertise.* Table D.2 lists three faculty as covering Software Security. However, this is not a main research area for any of them. The program would benefit from having a researcher working mainly in this area with expertise in, e.g. compilers and languages. This area would be a top priority in when hiring the six new faculty to deliver the program.
- *Competing teaching needs.* Many of the core faculty have expertise that is needed for BCS courses. In addition, two of the core faculty are Instructors, i.e. teaching faculty, who specialize in first and second year courses and will likely only be able to teach one course per year for the BCyber. See section D.4 below for more on this.
- *Retirements.* At this point, it is likely that three of the core faculty will retire before the program starts offering the new fourth-year courses. These faculty will need to be replaced by new hires with the required expertise.

- *Gender balance and diversity*. Three of the eleven core faculty identify as women. We do not have any other information on self-identification with classifications prioritized in Carleton's EDI efforts. The School is committed to doing its part in these efforts, and is particularly interested in making more progress on improving its gender balance.

### New faculty resources

The BCyber program requires eight new course offerings per year. The standard teaching load for tenure-track faculty in SCS is one graduate and two undergraduate courses per year. Because of the difficulty of finding contract instructors to teach third-year and fourth-year security courses, we need to factor in sabbaticals and other teaching release, and so five new tenure-track security faculty are needed for the new courses. In addition, as the BCyber contains most of the BCS core, enrolment in existing BCS courses will increase. Even with the current large section sizes of BCS core courses, we will require at least two more sections overall to accommodate BCyber students.

The university has approved in principle the hiring of the needed six tenure-track faculty members, at least five of which specialize in security, to support the program. The Dean will work with the unit to determine the hiring trajectory but provisional agreement has been given to hire 1 in year 2 of the program, 1 in year 3, and 2 in years 4, and 5. In addition, an Instructor (teaching-track faculty) will be hired in year 1 for a two-year term to 1) back-fill in the BCS for core faculty that will teach BCyber courses in the second year of the program, 2) help with the preparation of course materials for later courses, and 3) assist with the additional teaching load imposed on core BCS courses. The university has also approved the hiring of 2 contract instructors in years 1-6, as well as the funding for TAs (18 in year 1, 22 in year 2, 27 in year 3, 45 in year 4, 19 in year 5 and 40 in year 6). All hires for this program will be allocated by the Dean the Faculty of Science. Funding of positions and resources approved beyond the initial start of the program are based on student enrolment targets and will depend on meeting those enrolment targets. Positions and resources must be sought through the appropriate channels and are subject to university approvals.

## D.2. Faculty research funding

There are no plans for direct use of faculty research funds. While some of the advanced BCyber courses will likely involve student projects related to the research program of the course instructor, research funds will not be needed.

Nevertheless, we include a table summarizing core faculty research funding.

Table D.3 Faculty research funding

| | Canadian Industry | Federal Government (excluding Tri-Council, CRC, CFI, NCE) | Internal (Carleton) Grants/ Awards | Ontario (including OCE and MRI) | Tri-Agency (including CRC) | Total |
|---|---|---|---|---|---|---|
| **2018** | $40,000 | | $17,000 | $20,000 | $324,000 | **$401,000** |
| **2019** | | | $85,000 | | $450,000 | **$535,000** |
| **2020** | $65,000 | | $195,500 | | $268,825 | **$529,325** |
| **2021** | $215,000 | $50,000 | | | $377,660 | **$642,660** |
| **Total** | **$320,000** | **$100,000** | **$312,500** | **$20,000** | **$1,420,485** | **$2,172,985** |

## D.3. Distribution of thesis supervision

We do not discuss the current or planned distribution of thesis supervisions since the BCyber requires neither a thesis nor a capstone project. Instead, students will complete substantial projects in their advanced security courses. The supervision of the projects will be considered as part of the usual course workload.

## D.4. Recent teaching assignments

Table D.4 gives the teaching assignments of the core faculty over the last three years. All of the core faculty have had 100% of their teaching responsibilities allocated to the BCS and the grad programs run by the School of Computer Science, namely the MCS, PhD Computer Science, HCI Masters and Data Science Masters.

Table D.4 Recent UndergraduateTeaching Assignments

| Instructor | Course number | Sections taught | Course title |
|---|---|---|---|
| Abdou | COMP 3203 | 3 | Principles of Computer Networks |
| | COMP 4108 | 4 | Computer Systems Security |
| Barrera | COMP 3109 | 1 | Applied Cryptography and Authentication |
| | COMP 4000 | 1 | Distributed Operating Systems |
| | COMP 4109 | 1 | Applied Cryptography |
| | COMP 4108 | 2 | Computer Systems Security |
| Biddle | COMP 3008 | 1 | Human-Computer Interaction |
| Chiasson | COMP 3008 | 1 | Human-Computer Interaction |
| Hinek | COMP 1405 | 2 | Intro to Computer Science I |
| | COMP 1406 | 10 | Intro to Computer Science II |
| | COMP 2402 | 2 | Abstract Data Types/Algorithms |
| | COMP 3109 | 4 | Applied Cryptography and Authentication |
| Laurendeau | COMP 2401 | 4 | Intro to Systems Programming |
| | COMP 2404 | 7 | Intro to Software Engineering |
| | COMP 4203 | 1 | Wireless Networks & Security |
| Somayaji | COMP 1601 | 1 | Intro to Mobile Application Development |
| | COMP 2601 | 2 | Mobile Applications |
| | COMP 3000 | 7 | Operating Systems |
| | COMP 4000 | 2 | Distributed Operating Systems |
| | COMP 4501 | 1 | Real-Time Games |
| Stobert | COMP 3008 | 1 | Human-Computer Interaction |
| | COMP 3301 | 1 | Technical Writing for Computer Science |

| | | | |
|---|---|---|---|
| Van Oorschot | COMP 2109 | 1 | Intro to Security and Privacy |
| | COMP 4108 | 1 | Computer Systems Security |
| Zhao | COMP 3000 | 22 | Operating Systems |

We provide the following information to elaborate on Table D4.

- Chiasson and Van Oorschot held Canada Research chairs with a reduced teaching load.
- Others with a teaching load below the School norm of 2 undergrad and 1 undergrad course per year started at Carleton partly through the period covered by this data and had a reduced teaching load for their first few terms.
- Hinek and Laurendeau are teaching-track faculty with course loads of 6 and 5 respectively.
- The large number of COMP 3000 sections for Somayaji and Zhao is because they preferred to teach the class in a way that involved breaking it into unusually small sections.
- COMP 4109 and COMP 3109 are the same course. The course number was changed to be in line with the School's guidelines: courses at the 3000 and 4000 levels are all advanced courses, with degree of specialization being the main difference, while 3000-level courses correspond to "top-level" sub areas of CS, like graphics, operating systems and AI. COMP 4108 has also been moved to the 3000-level. COMP 3109 has been moved again, now to the 2000 level.
- A few of the security course sections were taught by contract instructors.

Table D.2 can be viewed as comprising two categories of courses currently taught by core faculty.

1. Second-year courses required in the BCS. These are all taught by Hinek and Laurendeau, the two teaching-stream faculty. Van Oorschot teaches a second year course, but it is an elective in the BCS core and is a security course that is required in the BCyber.
2. BCS advanced courses, i.e. COMP courses 3000 and above.

The point of the above breakdown is that back-filling BCS needs, when undergrad teaching of research-stream core faculty is shifted to BCyber courses, requires hiring new research-stream faculty with the expertise needed for the advanced BCS courses. There is currently no excess capacity: all the faculty with expertise in these areas are fully occupied teaching courses which are not part of the BCyber but are needed for the BCS. In other words, it is not possible to deliver the program by simply moving security faculty to the new courses and backfilling with contract instructors and generalist teaching-stream faculty.

In addition to the undergrad teaching noted above, all research-stream faculty teach a grad course of their choosing every year, independently of the needs of undergrad programs. The following table gives the grad courses taught by the core faculty in the last

Table D.5 Recent Graduate Teaching Assignments

| Instructor | Sections taught | Course title |
|---|---|---|
| Abdou | 4 | Internet Measurements&Security |
| Barrera | 2 | Operating Systems Security |
| | 2 | Internet of Things Security |

| | | |
|---|---|---|
| Chiasson | 1 | Comp. Security and Usability |
| Somayaji | 2 | Distributed Operating Systems |
| | 1 | Adaptive Security |
| Stobert | 2 | HCI: Models, Th. & Frameworks |
| Van Oorschot | 1 | Internet of Things Security |
| | 1 | Authentication & Software Sec |
| Zhao | 4 | Trusted Comp & Emerging Attack |

## D.5. Contract instructors

The courses specific to the BCyber will not use contract instructors, and none are asked for in the business plan submitted to the university. Staffing of courses from the BCS is the domain of the BCS governance and is beyond the scope of this document. Details can be found in the recent internal cyclical review of the BCS.

# E. Program Admission and Enrolment

## E.1. Admissions requirements

Since the BCyber is built from the Computer Science core, we use the same admission requirements as for the BCS, with the following modifications.

1. The minimum entrance average from Ontario high schools is raised to 85% from 70%. The 70% in the current calendar entry for the BCS is outdated. The *de facto* minimum for the BCS has been at least 80% for a number of years. The BCyber adds 5% to this mainly because of the compressed nature of first year, which has a fast-paced introduction to programming in the first term. Another reason is to position the program relative to competitors like Waterloo. Waterloo, though it has 80% calendar minimum, is well known to have a *de facto* minimum of 95%.
2. The BCS requires one of the 12U math courses *Calculus and Vectors* and *Advanced Functions.* The BCyber requires both to be in line with the admissions requirements of top competitors.

See Appendix 3 for the calendar language for the admission requirements.

## E.2. Class sizes and course and program capacity

There are three limiting factors for the size and capacity of the program.

1. A major goal of the program goal is to instil a strong sense of cohort. One of the distinguishing features of the BCyber that will help attract top students to the program is the opportunity to work closely with other future leaders of Canada's cybersecurity community. We have no hard data on what the right size is to achieve this goal, but we believe that it would become difficult if enrolment exceeds around 50 students per cohort.

2. As discussed in Section B, the six 4000-level ("fourth-year") courses in security will typically be based on projects with intensive involvement of the faculty member who is teaching the courser. Projects will often be related to the current research of the instructor. If we are to keep project management at a reasonable level of faculty work-load, enrolment should be under 50.
3. We plan accept upper-year admissions to the program only in rare cases. This is partly due to the goal of having a cohort-based student experience, and partly due to the uniqueness of the academic progression of the program. The course sequence has been carefully thought out and has prerequisite chains that would be difficult for students from other institutions to break into, largely because of lack of appropriate courses at the appropriate level.

Our initial plan is to admit 56 students per year (except for the first two years), and only into the first year of the program.

If we are able to recruit students of the calibre we expect, the retention rate should be high. The business plan submitted to the university shows an intake of 56 in first year flowing through to 47 in fourth year.

## E.3. Projected enrolment

Table E.1 gives the projected enrolment for the first six years of the program. The first-year intake in years 1 and 2 of the program are intended to be conservative predictions of intake while the program is being established and publicized. Cohort years beyond the first assumes the following retention rates: 92% first to second year; 87% second to third; 81% third to fourth.

Table E.1 Projected enrolment first six years

| | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 |
|---|---|---|---|---|---|---|
| **First year** | 46.0 | 51.0 | 56.0 | 56.0 | 56.0 | 56.0 |
| **Second year** | | 42.1 | 46.7 | 51.2 | 51.2 | 51.2 |
| **Third year** | | | 38.9 | 43.1 | 47.3 | 47.3 |
| **Fourth year** | | | | 38.9 | 43.1 | 47.4 |
| **Total** | 46.0 | 93.1 | 141.5 | 189.3 | 197.7 | 201.9 |

# F. Student Experience and Satisfaction

## F.1. Student orientation, advising, and mentoring

Routine student advising for the BCyber will be provided by the BCS undergrad advising staff. There are currently three staff members. We are requesting resourcing for additional staff time for the additional advising load. All of the advising staff members will be trained on the new program.

The SCS website has an extensive section with information for current students (here). This includes course outlines, technical help for the School's computing resources, and help with registration and

course selection. Most of this will apply as-is to BCyber students. Some parts, such as course selection, will be augmented with BCyber-specific information.

One of the features of the BCyber is the cohort experience for students. We will start this a separate orientation for the BCyber where students can meet the security faculty and some current students.

The cohort experience will be maintained partly through specific courses and course registration planning distributed through the years of the program.

1. In first year, students will take the "compressed" version of two introductory courses (see section B.3 for more on this). This course will be small since it will be restricted to BCyber students and students in our Internship option.
2. In second year, students will take COMP 2109 *Introduction to Security and Privacy* and CYB 2108 *Applied Cryptography and Authentication.* COMP 2109 is an introductory course that is offered to all BCS students. It is optional for BCS students but required for BCyber students. Based on recent experience it is likely that about half the course will be made up of BCyber students. CYB 2108 will be restricted to BCyber students.
3. In third year and fourth year, BCyber students will CYB 3108 *Systems Security,* an introduction to the field restricted to BCyber students. They will also take six required fourth-year courses in security, all of which will have enrolment limited to 40 or so, implying that most of the students will be in the BCyber. Students following the recommended course pattern will take two of these fourth-year courses in third year.

## F.2. Career paths of graduates

The job prospects for BCS graduates are overall exceptionally strong, witness the vast numbers flocking into CS programs nationwide. Since growth in the need for security specialists in the IT sector has far outstripped the overall growth of the sector, the market for graduates with both software developer and security competencies is even stronger.

Because the BCyber has a large overlap with the standard Computer Science bachelor's degree, all of the career paths open to BCS graduates, including graduate studies in Computer Science, are also open to BCyber graduates. In addition, BCyber graduates will have strong preparation for leadership positions in industry and government that have a focus on security. Security is a major concern for most software development, so many of the usual software roles have variants that specialize in security. There are also roles particular to systems/software/IT security.

The Cybersecurity and Infrastructure Security Agency of the United States has a division NICCS (National Initiative for Cybersecurity Careers and Studies) dedicated to the training and placement of cybersecurity professionals. The NICCS website has extensive material on career paths for graduates of security programs. These include the following.

- Data Analyst
- Database Administrator
- Enterprise Architect
- Knowledge Manager
- Network Operations Specialist
- Research & Development Specialist
- Software Developer

- System Administrator
- System Testing and Evaluation Specialist
- Systems Developer
- Systems Requirements Planner
- Technical Support Specialist
- Research and Development Specialist
- Communications Security (COMSEC) Manager
- Cyber Defense Analyst
- Cyber Defense Forensics Analyst
- Cyber Defense Incident Responder
- Cyber Defense Infrastructure Support Specialist
- Information Systems Security Developer
- Information Systems Security Manager
- Secure Software Assessor
- Security Architect
- Security Control Assessor
- Systems Security Analyst
- Vulnerability Assessment Analyst

## F.3. Co-op

We have designed a course pattern that BCyber students will be strongly steered towards. The pattern is derived from the one used for the BCS Industrial Internship Option. The pattern is designed to "front load" the course sequencing with courses deemed especially useful for co-op work so that students can have a more meaningful first co-op placement at the end of their second year.

What enables this front-loading is a compressed introduction to programming. It comprises two courses (COMP 1405 and COMP 1406) that are normally taken over the fall and winter semesters. BCyber students instead will take the two courses over Carleton's two fall "half-terms". The content and workload is the same. The only difference is that each course has half the elapsed time.

Below is the full course pattern.

BCSec Recommended Course Pattern

| | **Year 1** | **Year 2** | **Year 3** | **Year 4** |
|---|---|---|---|---|
| **Fall** | COMP 1405&1406<br>Programming I&II | COMP 2109<br>Security & Privacy | COMP 2804<br>Discrete Math II | CYB4000/1/2/3<br>OS/HF/Net/Soft |
| | COMP 1805<br>Discrete Math I | COMP 2402<br>Data Structures | COMP 3008<br>HCI | CYB 4900<br>Security Topics I |

| | Year 1 | Year 2 | Year 3 | Year 4 |
|---|---|---|---|---|
| | MATH 1007<br>Calculus | COMP 2404<br>Software Eng. | CYB 3108<br>Systems Security | Elective |
| | Elective | MATH 1104<br>Linear Algebra | Elective | Elective |
| | — | Elective | Elective | Elective |
| **Winter** | COMP 2401<br>Systems Prog. | CYB 2108<br>Cryptography | CYB4000/1/2/3<br>OS/HF/Net/Soft | CYB4000/1/2/3<br>OS/HF/Net/Soft |
| | COMP 2406<br>Web Applications | COMP 3000<br>Operating System | CYB4000/1/2/3<br>OS/HF/Net/Soft | CYB 4901<br>Security Topics II |
| | STAT 2507<br>Statistical Modeling | COMP 3004<br>OO Software Eng. | Elective | Elective |
| | Elective | COMP 3203<br>Networks | Elective | Elective |
| | Elective | Elective | Elective | Elective |

**Notes:**
**-** The electives must include at least two of: MATH 2108, COMP 3002, COMP 3301, COMP 4004, COMP 4203.
- Students are encouraged to take further technical electives, including in MATH, that support their chosen areas of interest or specialization.

# G. Resources.

## G.1. Support and technical staff

### Support Staff

The School's three Undergraduate Program Advisors are staff members dedicated to the undergraduate programs offered by the School. They organize, advise and perform the necessary administrative duties required for all the students in the School's undergraduate programs. They advise students on required courses for their program, advise transfer students about program adjustments, and assist special students and other non-BCS students wanting to take undergraduate computer science courses. They determine students' eligibility for promotion, continuation, and awards.

### Technical Staff

We have five regular technical staff members supporting the computing infrastructure and labs for the undergraduate programs offered by the school

1. The manager of Technical Operations is in charge of the technical staff. They are also responsible for the cloud storage platform, and network security and offer various technical services to faculty members.

2. The Senior Software Designer is responsible for the virtualization platform and virtual machines customized for every course.
3. The Software Designer is responsible for the provision, maintenance, and operation of software, cloud computing, and virtualization environments to support the teaching activities of the School. It includes installing and maintaining the hardware used for cloud computing and the virtualization of instructional and research resources. Other related primary activities include liaison with faculty regarding the use of instructional software and infrastructure; preparation of user documentation for faculty and students; support of researchers in using virtualization and adapting their code for those environments.
4. The Senior Systems Administrator is responsible for the web presence, Linux network administration, end-user documentation, supporting faculty, staff, and students, supporting research, and purchasing for the technical operations.
5. The Network Administrator is responsible for keeping the instructional laboratories in operational and good condition. They install and maintain the hardware and software, and troubleshoot hardware and network problems. They build, test, deploy and maintain the main system image containing the software required for all courses. They provide technical support to faculty members, admin staff, lab coordinators, and students.

### Lab Coordinators

We have five full-time Lab Coordinators. They manage the undergraduate tutorial/lab component of our courses. There duties include: leading many of the tutorial sessions; ensuring consistency and uniformity across sections; preparation, training and supervision of teaching assistants; monitoring the effectiveness of the laboratory exercises; assessing the need for changes in the laboratory course content; and running grading sessions for assignments and tests.

## G.2. Space

No new space is being added for this program, in the sense that all needs will be met from existing space allocations/pools of the university and the School. To assess the adequacy of this it is important to note the following.

- Like the BCS, the BCyber will have a laptop requirement: all students are required to have laptop that can run all the course software, and course instructors can require students to bring laptops to lectures, labs and tutorials.
- The university centrally supports CoMaS, an e-proctoring system developed in our School. Instead of locking down most of its host's functionality, it installs monitoring tools that are flexible enough to allow students to use whatever development environment they're most comfortable with.
- Course software is all free to students. They can install it on their own machines, or they can install course-specific pre-configured virtual machine images.
- The School's makes extensive use of cloud computing, managed using OpenStack. Researchers buying new equipment for their lab usually have it added to the cloud infrastructure. Most equipment funding for the BCS program is used for cloud upgrades/additions. Students are all given access to OpenStack. Some courses will have compute images for students to clone and run, but students are free to create their own (with some restrictions on network use).

There are five kinds of space relevant to the delivery of the program. We discuss each with reference to the above notes.

1. Classroom space. BCyber courses, like BCS courses, require no special classroom space. Lectures will use a combination of slides and live coding. For lectures requiring in-class programming exercises, students use their own laptops. The university has extensively upgraded its classrooms and is able to grant all requests for classroom space with this lecture style. Special spaces for quizzes and midterms is not needed. Some classes run quizzes in tutorials (see the next item). Typically, they are run during the lecture period, either online or in the classroom, using either paper or laptops with CoMaS.
2. Tutorial space. Many courses run "tutorials", i.e. labs of 80 students or less where students work through assigned exercises with TA support. Some tutorials are run online, and some use the School's dedicated tutorial space. Many students bring their own laptops to the tutorial room, but there are also 80 desktop PCs configured with all the needed course software. Tutorials taking place here usually do the course's quizzes there as well.
3. Workstation "labs". In addition to the tutorial room, the School has three undergraduate "open labs", i.e. rooms with PCs open to all BCS students. The BCyber will share these. The rooms have a total of 82 PCs. Their use is not required by any course. Courses like Operating Systems and Networks that require host root access use cloud instances. Specialized hardware, like GPUs for Machine Learning, is available through Openstack. Despite the small number of machines relative to the BCS enrolment (around 3000), the labs are not overloaded. Based on anecdotal evidence, the typical use cases for a student are 1) using a computer when they have some free time on campus but forgot to bring their laptop, or 2) physically meeting with the other students working on their team project.
4. Collaboration space. The School and Faculty of Science per se have very little of this. However, the university has been adding such space steadily over the years. The library has a substantial amount, both free and bookable, and there are large public spaces scattered around campus at the tunnel level, on the main floors of buildings, and in the University Center.
5. Faculty research labs. Some of the advanced CYB courses may involve work within the instructor's research program. We expect that even in such courses, the number of students needing physical access to the instructor's lab will be tiny.

## G.3. Library Resources

We expect the library to play the same role in the BCyber as in the BCS. Almost all reference material in courses will be freely available on the web. The web will also be the primary resource for students wanting to explore beyond the boundaries of their courses.

The main use of the library will be in advanced courses, which may require reference to recent research articles. The Library has electronic subscriptions covering all major publication venues, both journals and conferences, in computer science and security.

An analysis of Carleton University Library's information resources and services in support of the program demonstrates that the Library does not require additional funds to support it. The Library's collection includes specific resources to support the proposed program. The full report from the Library is included as Appendix 4.

The Library report is prepared by the librarian or subject specialist responsible for the subject area(s) covered by the program, using a common template developed from guidelines established by the Ontario Council of University Libraries. The main purpose of the report is to specify whether any new resources or services are necessary in order to support the program, for example, whether the Library needs to purchase new books or subscribe to new journals or electronic resources.

The librarians and subject specialists preparing the reports rely on their own professional experience with collecting resources in the subject areas in order to make assessments about whether there are

gaps in the collection that need to be filled in order to provide the appropriate teaching and research support for new, modified, or reviewed programs. They consult various sources for information about published resources in the subject area, including the database maintained by the Library's main monographs vendor, publishers' lists and websites, handbooks and guides to the literature, the library collections of universities that offer the program, various specialized sites relevant to the subject from professional societies and organizations, as well as basic information available in tools such as Google Scholar or generally on the web. They also generally consult faculty members (e.g., the Library representative or the department chair) to discuss their assessment of the strengths and gaps. The Library makes a clear distinction between those resources which are essential to the program and those which are simply "nice to have." Generally speaking, the reports list only the essential resources, with costing obtained from the vendors or agents from which the Library would obtain the materials: each item is listed and costed individually and the total amount is recorded in the report.

The report also provides context by providing information about the following, when possible or applicable: percentage of top-ranked journals which the Library subscribes to in the subject area(s); how much funds have been spent in the past fiscal year on e-resources, journals, and printed books in support of the subjects covered by the program; how much funds have been spent in the past 8 years on printed monographs for the program; specialized collections in archives, maps, data, and government information; instruction, teaching, and practicums carried out by Library staff in the classroom or in the Library; highlights from the Library website (e.g., links for subject and course guides and to online tutorials); research partnerships between the Library and the department or program; research consultations; help desk visits; and selected detailed statistical information about the Library.

# H. Development of the Self-Study

With the exception of the Library's report, the Paul Menton Centre report, and Section G.1, the assessment was written by Douglas Howe, a Professor in the School of Computer Science. The writing was done in close collaboration with Paul Van Oorschot, the School's Tier I CRC in security. Van Oorschot conceived the program and worked with the other security faculty in the School to design the curriculum. He is a recognized expert in security education: see, for example, his paper "A view of security as 20 subject areas in four themes", published in IEEE Security & Privacy 20(1):102-108. A non-paywalled version of the paper can be found here.

The data used in this report's tables was obtained mostly from the university's Office of Institutional Research and Office of the Vice-President of Research and International. The Library and the Paul Menton Centre for Students with Disabilities contributed reports that have been included verbatim here.

# Appendix 1. Calendar specification - program

Below is the calendar language for the BCyber program. The courses with course code CYB are all new. All COMP, MATH and STAT courses are currently in the calendar. For the current calendar descriptions of existing BCS programs, see the calendar website.

## BCyber Honours (20.0 credits)

### *Credits Included in the Major CGPA (11.5 credits)*

1. *5.0 credits in:*
   COMP 1405 [0.5] Introduction to Computer Science I
   COMP 1406 [0.5] Introduction to Computer Science II
   COMP 1805 [0.5] Discrete Structures I
   COMP 2401 [0.5] Introduction to Systems Programming
   COMP 2402 [0.5] Abstract Data Types and Algorithms
   COMP 2404 [0.5] Introduction to Software Engineering
   COMP 2406 [0.5] Fundamentals of Web Applications
   COMP 2804 [0.5] Discrete Structures II
   COMP 3000 [0.5] Operating Systems
   COMP 3004 [0.5] Object-Oriented Software Engineering

2. *2.5 credits in:*
   CYB 2108 [0.5] Applied Cryptography and Authentication
   COMP 2109 [0.5] Introduction to Security and Privacy
   COMP 3008 [0.5] Human-Computer Interaction
   COMP 3203 [0.5] Principles of Computer Networks
   CYB 3108 [0.5] Computer Systems Security

3. *1.0 credits from:*
   MATH 2108 Abstract Algebra
   COMP 3301 Technical Writing for Computer Science
   COMP 3002 Compiler Construction
   COMP 4004 Software Quality Assurance
   COMP 4203 Wireless Networks and Security

4. *3.0 credits from:*
   CYB 4000 Operating Systems Security
   CYB 4100 Human Factors in Security
   CYB 4200 Network Security
   CYB 4300 Software Security
   CYB 4900 Advanced Topics in Security I
   CYB 4901 Advanced Topics in Security II

### *B. Credits Not Included in the Major CGPA (8.5 credits)*

6. *1.0 credit from:*
   MATH 1007 [0.5] Elementary Calculus I
   MATH 1104 [0.5] Linear Algebra for Engineering or Science

7. *0.5 credit in:*
   STAT 2507 [0.5] Introduction to Statistical Modeling I

8. 7.0 *credits of Free Electives*

# Appendix 2. Calendar specification - courses

Below is the calendar language for the new courses in the BCyber. The courses with course code CYB are all new. All COMP, MATH and STAT courses are currently in the calendar. We include the current calendar listings for existing courses that are used in the BCyber. For a complete listing of current Carleton courses, see the calendar website.

## COMP (Computer Science)

**COMP 1405 [0.5 credit]**
**Introduction to Computer Science I**
Introduction to computer science and programming, for computer science students. Topics include: algorithm design; control structures; variables and types; linear collections; functions; debugging and testing. Special attention is given to procedural programming in a modern language, computational thinking skills, and problem decomposition.
Includes: Experiential Learning Activity
Precludes additional credit for BIT 1400, CGSC 1005, COMP 1005, ECOR 1041, ECOR 1042, ECOR 1051, ECOR 1606, ITEC 1400, ITEC 1401, SYSC 1005.
Prerequisite(s): restricted to students registered in the B.C.S. program, combined Honours in Computer Science and Mathematics, Honours Computer Mathematics, and Honours Computer Statistics.
Lectures three hours a week, tutorial one and a half hours a week.

**COMP 1406 [0.5 credit]**
**Introduction to Computer Science II**
A second course in programming for BCS students, emphasizing problem solving and computational thinking in an object-oriented language. Topics include abstraction, mutable data structures, methods, inheritance, polymorphism, recursion, program efficiency, testing and debugging.
Precludes additional credit for BIT 2400, BUSI 2402, COMP 1006, ITEC 2400, ITEC 2401, SYSC 2004.
Prerequisite(s): COMP 1005 or COMP 1405.
Restricted to students registered in the B.C.S. program, combined Honours in Computer Science and Mathematics, Honours Computer Mathematics, and Honours Computer Statistics.
Lectures three hours a week, tutorial one and a half hours a week.

**COMP 1805 [0.5 credit]**
**Discrete Structures I**
Introduction to discrete mathematics and discrete structures. Topics include: propositional logic, predicate calculus, set theory, complexity of algorithms, mathematical reasoning and proof techniques, recurrences, induction, finite automata and graph theory. Material is illustrated through examples from computing.
Includes: Experiential Learning Activity
Precludes additional credit for MATH 1800. Prerequisite(s): one Grade 12 university preparation mathematics course.
Lectures three hours a week, tutorial one hour a week.

**COMP 2109 [0.5 credit]**
**Introduction to Security and Privacy**
A tour of Internet security and privacy. Societal impacts and case studies. Topics from: protection goals of stakeholders; history of public key cryptography; programming languages and security; security engineering and testing; cybercrime and malware; Internet privacy and anonymity; government surveillance; regulation; ethics; blockchain applications.
Includes: Experiential Learning Activity
Prerequisite(s): COMP 1406 with a minimum grade of C-, and COMP 2401 with a minimum grade of

C-.
Lectures three hours a week.

**COMP 2401 [0.5 credit]**
**Introduction to Systems Programming**
Introduction to system-level programming with fundamental OS concepts, procedures, primitive data types, user-defined types. Topics may include process management, memory management, process coordination and synchronization, inter-process communication, file systems, networking, pointers, heap and stack memory management, and system/library calls.
Precludes additional credit for SYSC 2006. Prerequisite(s): (COMP 1006 or COMP 1406 or SYSC 2004) with a minimum grade of C-.
Lectures three hours a week, tutorial one and a half hours a week.

**COMP 2402 [0.5 credit]**
**Abstract Data Types and Algorithms**
Introduction to the design and implementation of abstract data types and to complexity analysis of data structures. Topics include: stacks, queues, lists, trees and graphs. Special attention is given to abstraction, interface specification and hierarchical design using an object- oriented programming language.
Precludes additional credit for SYSC 2100. Prerequisite(s): (COMP 1006 or COMP 1406 or SYSC 2004) with a minimum grade of C-.
Lectures three hours a week.

**COMP 2404 [0.5 credit]**
**Introduction to Software Engineering**
Introduction to object-oriented software development, with emphasis on the design and implementation of maintainable, reusable software. Topics include abstraction, modularity, encapsulation, and an introduction to design patterns.
Includes: Experiential Learning Activity
Precludes additional credit for SYSC 3010, SYSC 3110.
Prerequisite(s): COMP 2401 with a minimum grade of C-.
Lectures three hours a week, tutorial one and a half hours a week.

**COMP 2406 [0.5 credit]**
**Fundamentals of Web Applications**
Introduction to Internet application development; emphasis on computer science fundamentals of technologies underlying web applications. Topics include: scripting and functional languages, language-based virtual machines, database query languages, remote procedure calls over the Internet, and performance and security concerns in modern distributed applications.
Includes: Experiential Learning Activity
Precludes additional credit for SYSC 4504.
Prerequisite(s): (COMP 1006 or COMP 1406 or SYSC 2004) with a minimum grade of C-.
Lectures three hours a week and tutorial one and a half hours a week.

**COMP 2804 [0.5 credit]**
**Discrete Structures II**
A second course in discrete mathematics and discrete structures. Topics include: counting, sequences and sums, discrete probability, basic statistics, recurrence relations, randomized algorithms. Material is illustrated through examples from computing.
Prerequisite(s): COMP 1805 with a minimum grade of C-, or permission of the School of Computer Science for those in Combined Honours in Computer Science and Mathematics.
Lectures three hours a week.

**COMP 3000 [0.5 credit]**
**Operating Systems**
Operating system implementation course stressing fundamental issues in design and how they relate to modern computer architectures. Assignments involve the modification and extension of a

multitasking operating system.
Includes: Experiential Learning Activity
Precludes additional credit for SYSC 4001.
Prerequisite(s): COMP 2401 with a minimum grade of C- and (COMP 2402 or SYSC 2100).
Lectures three hours a week, tutorial one and a half hours a week.

**COMP 3002 [0.5 credit]**
**Compiler Construction**
The structure, organization and design of the phases of a compiler are considered: lexical translators, syntactical translators, scope handlers, type checkers, code generators and optimizers. Components of a compiler will be implemented.
Prerequisite(s): (COMP 2402 or SYSC 2100).
Lectures three hours a week.

**COMP 3004 [0.5 credit]**
**Object-Oriented Software Engineering**
Development of object-oriented software systems: theory and practice. Topics include: Computer ethics, software development processes, requirement specification, class and scenario modeling, state modeling, UML, design patterns, traceability. Students are to complete a team project.
Includes: Experiential Learning Activity
Precludes additional credit for SYSC 3020, SYSC 3120, SYSC 4120.
Prerequisite(s): COMP 2401 with a minimum grade of C-, (COMP 2404 or SYSC 3010 or SYSC 3110) with a minimum grade of C-, and (COMP 2406 or SYSC 4504).
Lectures three hours a week.

**COMP 3008 [0.5 credit]**
**Human-Computer Interaction**
Fundamentals of the underlying theories, design principles, development and evaluation practices of human-computer interaction (HCI). Topics may include: theories of interaction, user interface frameworks, desktop, web, mobile, and immersive applications, usability inspection and testing methods, and qualitative and quantitative approaches to HCI research.
Prerequisite(s): (COMP 2404 or SYSC 3010 or SYSC 3110) and (COMP 2406 or SYSC 4504).
Lectures three hours a week.

**COMP 3203 [0.5 credit]**
**Principles of Computer Networks**
This is an introductory course to the field of Network Computing. Topics include: Protocol Architectures and Internetworking, Types of Networks, Communication Protocols, End-System and Network Traffic Management, Structure of Routing and Congestion Control.
Includes: Experiential Learning Activity
Precludes additional credit for SYSC 4602. Prerequisite(s): COMP 2401 with a minimum grade of C-, and (COMP 2402 or SYSC 2100).
Lectures three hours a week.

**COMP 3301 [0.5 credit]**
**Technical Writing for Computer Science**
Technical communication for computer science majors, concentrating on writing scientific papers and technical reports. Principles of clarity and precision in writing and communication. Practical exercises and readings from recent technical publications will be used.
Prerequisite(s): (COMP 2402 or SYSC 2100) and (COMP 2404 or SYSC 3010 or SYSC 3110).
Lectures three hours a week.

**COMP 4004 [0.5 credit]**
**Software Quality Assurance**
Introduction to the theory and practice of Software Quality Assurance. Topics include: equivalence partitioning, test- driven testing, unit testing patterns, refactoring, software metrics, requirements engineering, scenario modeling and acceptance testing, model-based testing, state machine testing,

software testing theory and tools.
Precludes additional credit for SYSC 4101.
Prerequisite(s): COMP 3004.
Lectures three hours a week.

**COMP 4203 [0.5 credit]**
**Wireless Networks and Security**
An introduction to wireless networks covering both networking issues and security aspects of modern wireless environments. Fundamentals of mobile LANs, ad hoc, sensor networks, secure routing, searching, clustering, multicasting, localization, mobile IP/TCP, confidentiality, key establishment, authentication, broadcasting, RFIDs, and rogue attacks.
Prerequisite(s): COMP 3203 or SYSC 4602.
Lectures three hours a week.

# CYB (Cybersecurity)

**CYB 2108 [0.5 credit]**
**Cryptographic Algorithms and Protocols**
Block ciphers and modes of operation; public-key encryption; cryptographic hash functions; digital signatures; password-based cryptography; randomness and guesswork; authentication and authenticated key establishment protocols; challenge-response protocols; elliptic curve cryptography; post-quantum algorithms.
Includes: Experiential Learning Activity
Precludes additional credit for COMP 2018, COMP 3109 (no longer offered), COMP 4109 (no longer offered).
Prerequisite(s): COMP 1406 with a minimum grade of C-, MATH 1104 and either COMP 2804 or STAT 2507.
Lectures three hours a week, tutorials one and a half hours a week.

**CYB 3108 [0.5 credit]**
**Systems Security**
Securing networked computer systems. Threat modelling. Operating system security and design principles; access control. Software-based exploits, memory safety, non-functional testing in software development. Social engineering. Browser-server and transport-layer security. Middleperson attacks, end-to-end security. Public-key certificates. Case study: Bluetooth or Wi-Fi security.
Includes: Experiential Learning Activity
Precludes additional credit for COMP 4108, SYSC 4810.
Prerequisite(s): CYB 2108, (COMP 3000 or SYSC 4001), and COMP 3203.
Lectures three hours a week, tutorials one and a half hours a week.

**CYB 4000 [0.5 credit]**
**Operating Systems Security**
The course examines past, present, and emerging approaches for securing operating systems. The focus is to provide a foundation for understanding requirements to secure hosts at the operating system level and survey the landscape of available tools and techniques for implementing operating system security controls.
Includes: Experiential Learning Activity
Prerequisites(s): COMP 3000, CYB 3108
Lectures three hours a week.

**CYB 4100 [0.5 credit]**
**Human Factors in Security**
Designing security mechanisms with human factors in mind. Evaluating software-based systems

with focus on how interaction design affects security and privacy. Current approaches to usable security; user studies; methodologies for empirical analysis; design principles for usable security and privacy; case studies including authentication, anonymity systems.
Includes: Experiential Learning Activity
Prerequisites(s): COMP 3008 (HCI), CYB 3108
Lectures three hours a week.

**CYB 4200 [0.5 credit]**
**Network Security**
Security throughout network stack layers. Internet core security. VPNs and tunnelling protocols. Firewalls and Intrusion Detection Systems. Internet measurements. IoT security. Botnets. Securing network protocols, including email and web. Network monitoring. Traffic sniffers and vulnerability scanners.
Includes: Experiential Learning Activity
Prerequisites(s): COMP 3000, COMP 3203, CYB 3108
Lectures three hours a week.

**CYB 4300 [0.5 credit]**
**Software Security**
Resilience of everyday software to vulnerabilities. Security engineering and the security development lifecycle. Static analysis and vulnerability analysis. Model checkers. Security testing, non-functional testing, fuzz-testing. Programming languages and security. Cryptographic APIs and use of security toolkits.
Includes: Experiential Learning Activity
Prerequisites(s): COMP 3000, COMP 3004, CYB 3108
Lectures three hours a week.

**CYB 4900 [0.5 credit]**
**Advanced Topics in Security I**
An in-depth study of selected topics, with an emphasis on areas of strong current interest in research or practice. The selected topics will not have significant overlap with those in CYB 4901.
Prerequisites(s): CYB 3108; other prerequisites may be added depending on the topics.
Lectures three hours a week.

**CYB 4901 [0.5 credit]**
**Advanced Topics in Security II**
An in-depth study of selected topics, with an emphasis on areas of strong current interest in research or practice. The selected topics will not have significant overlap with those in CYB 4900.
Prerequisites(s): CYB 3108; other prerequisites may be added depending on the topics.
Lectures three hours a week.

## MATH/STAT (Mathematics/Statistics)

**MATH 1007 [0.5 credit] Elementary Calculus I**
Limits. Differentiation of the elementary functions, including trigonometric functions. Rules of differentiation. Applications of differentiation: max-min problems, curve sketching, approximations. Introduction to integration: definite and indefinite integrals, areas under curves, fundamental theorem of calculus.
Precludes additional credit for BIT 1000, BIT 1100, BIT 1200, MATH 1002 (no longer offered), MATH 1004, MATH 1401/ECON 1401, MATH 1402/ECON 1402, MATH 1052.
Prerequisite(s): Ontario Grade 12 Mathematics: Advanced Functions; or MATH 0005 and MATH 0006; or equivalent.
Lectures three hours a week, tutorial one hour a week.

**MATH 1104 [0.5 credit]**
**Linear Algebra for Engineering or Science**

Systems of linear equations. Matrix algebra. Determinants. Invertible matrix theorem. Cramer's rule. Vector space R^n; subspaces, bases. Eigenvalues, diagonalization. Linear transformations, kernel, range. Complex numbers (including De Moivre's theorem). Inner product spaces and orthogonality. Applications.
Precludes additional credit for BIT 1001, BIT 1101, BIT 1201, MATH 1102 (no longer offered), MATH 1107, MATH 1119, MATH 1401/ECON 1401, MATH 1402/ECON 1402, MATH 1152. Note: MATH 1119 is not an acceptable substitute for MATH 1104.
Prerequisite(s): Ontario Grade 12 Mathematics: Advanced Functions, or MATH 0005, or equivalent, or permission of the School. Restricted to students in the Faculty of Engineering, the School of Computer Science, or in certain B.Sc. and B.A.S. programs where specified.
Lectures three hours a week and tutorial one hour a week.

**MATH 2108 [0.5 credit]**
**Abstract Algebra I**
Sets and relations, number theory, group theory, ring theory, cardinal numbers.
Precludes additional credit for MATH 3101 and MATH 2100.
Prerequisite(s): i) MATH 2152 or MATH 2107; and ii) MATH 1800 (MATH 1800 may be taken concurrently, with permission of the School); or COMP 1805; or permission of the School.
Lectures three hours a week and one hour tutorial.

**STAT 2507 [0.5 credit]**
**Introduction to Statistical Modeling I**
A data-driven introduction to statistics. Basic descriptive statistics, introduction to probability theory, random variables, discrete and continuous distributions, contingency tables, sampling distributions, distribution of sample mean, Central Limit Theorem, interval estimation and hypothesis testing. A statistical software package will be used.
Includes: Experiential Learning Activity
Precludes additional credit for BIT 2000, BIT 2009, BIT 2100 (no longer offered), BIT 2300 (no longer offered), ECON 2201 (no longer offered), ECON 2210, ENST 2006, GEOG 2006, STAT 2601, STAT 2606, and STAT 3502. May not be counted for credit in any program if taken after successful completion of STAT 2559.
Prerequisite(s): an Ontario Grade 12 university-preparation Mathematics or equivalent, or permission of the School of Mathematics and Statistics.
Lectures three hours a week, laboratory one hour a week.

# Appendix 3. Calendar specification - admission

Below is the calendar specification for the BCyber admissions requirements. For the current calendar entry for admission into BCS programs, see the calendar website.

## Admissions Information

Admission requirements are based on the Ontario High School System. Prospective students can view the admission requirements through the Admissions website at admissions.carleton.ca. The overall average required for admission is determined each year. Holding the minimum admission requirements only establishes eligibility for consideration.

Note: If a course is listed as recommended, it is not mandatory for admission. Students who do not follow the recommendations will not be disadvantaged in the admission process.

## Degree

Bachelor of Cybersecurity (BCyber) (Honours)

## Admission Requirements

### First Year

The Ontario Secondary School Diploma (OSSD) or equivalent, including a minimum of six 4U or M courses. The six 4U or M courses must include both *Advanced Functions* and *Calculus and Vectors*. An overall average of at least 85% is normally required to be considered for admission. Note that an average of 85% only establishes eligibility for consideration for admission; the minimum acceptable average will usually be significantly higher.

### Advanced Standing

Applications for admission beyond first year will be assessed on their merits. Students must typically present a minimum CGPA of 7.00 (B-) in order to be considered for admission. Applicants will likely need to complete the supplementary application process outlined above for first year admission.

### Co-op Option

For direct admission to the first year of the co-op option applicants must:

1. meet the required overall admission cut-off average and prerequisite course average; these averages may be higher than the stated minimum requirements;
2. be registered as a full-time student in the Bachelor of Cybersecurity program;
3. be eligible to work in Canada (for off-campus work placements).

Meeting the above requirements only establishes eligibility for admission to the program. The prevailing job market may limit enrolment in the co-op option.

Note: continuation requirements for students previously admitted to the co-op option and admission requirements for the co-op option after beginning the program are described in the Co-operative Education Regulations section of this Calendar.

## Appendix 4. Library report


# Institutional Quality Assurance Process

Library Report for Bachelor of Computer and Internet Security

New Program

*Date:* October 14, 2022

*Compiled by:* George Duimovich, Collections Librarian, Science, Engineering & Design Team

*Submitted to:* Alicia Hollington, Program Coordinator, Office of the Vice-Provost & Associate Vice-President (Academic)

*cc* Amber Lannon, University Librarian
Laura Newton Miller, Head of Collections & Assessment
Sally Sax, Head of Electronic Resources & Acquisitions
Patti Harper, Head of Research Support Services

## Overview and Recommendations

An analysis of Carleton University Library's information resources and services in support of the program demonstrates that the Library does not require additional funds to support it.

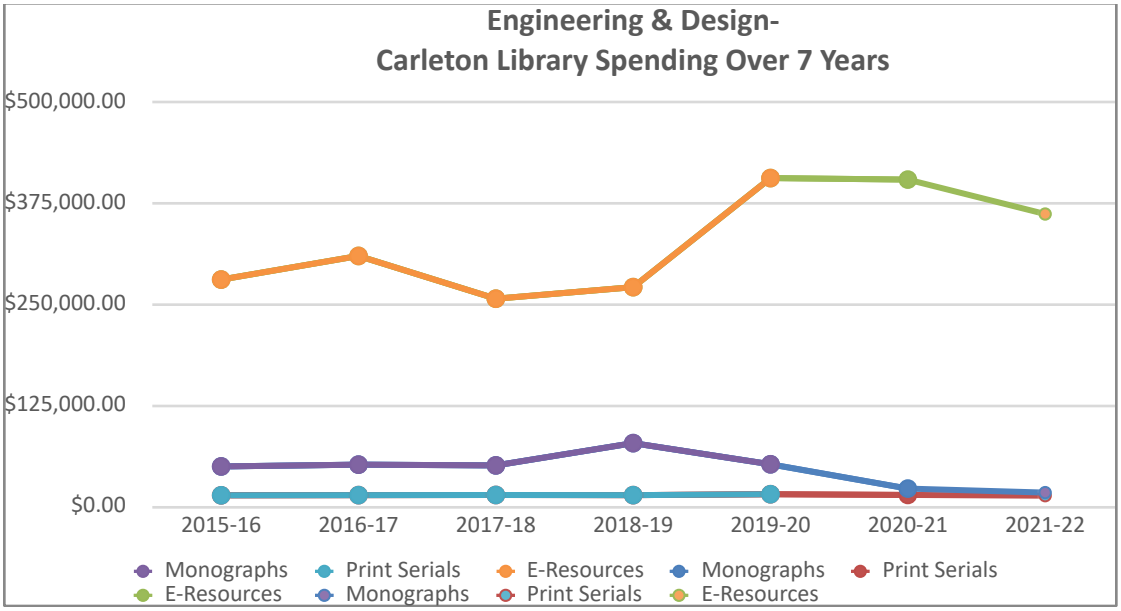
## Library Collections

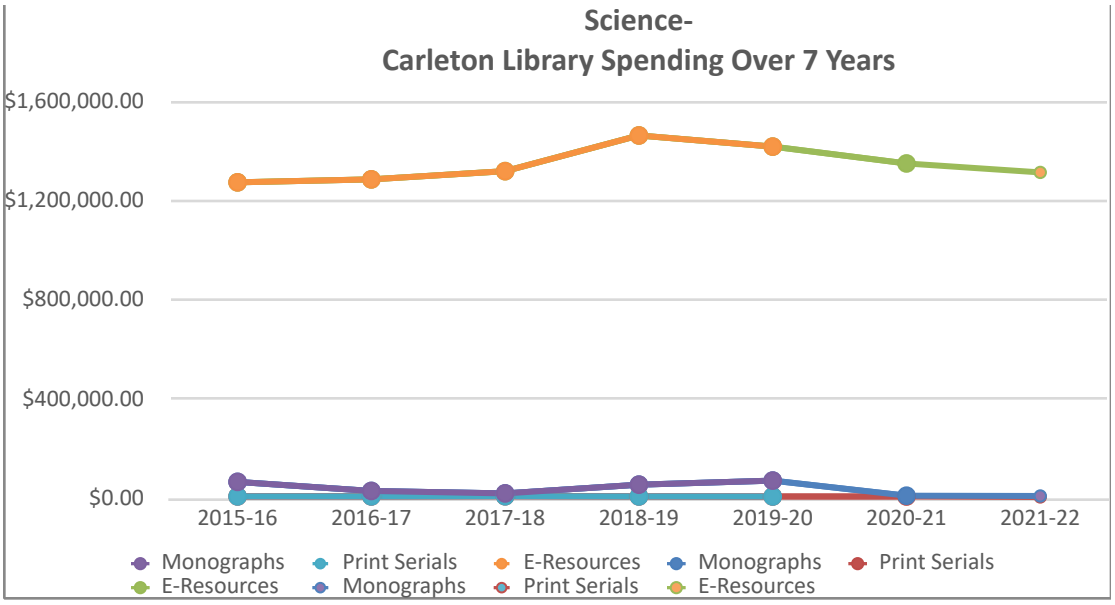
### Subject Specific

The Library's collection includes specific resources to support the Bachelor of Computer and Internet Security. These include 25 of the top-ranked 25 journals in Journal Citation Reports classified under the subject categories: Computer Science, Software Engineering as well as 20 of top 20 journals ranked in Google Scholar citations for computer / information security. In addition, the Library's collections of journals in related programs are also strong in Computer Science as well as Software Engineering, Information Technology and Mathematics.

During the 2021-2022 academic year, the Library's spending for collection in all areas was about $6.3 million. 88% of the entire collections budget is spent on electronic resources**.** Over $5.5 million was spent on general electronic resources which benefit all subject areas.

In addition to that amount, the following shows the amounts spent on electronic resources (databases, journals, ebook packages, indexes), print journals, and monographs (individual orders) related to Faculty of Engineering and Design and the Faculty of Science for the past seven years***:***






The policy for materials that the Library collects for the Bachelor of Computer and Internet Security may be found at https://library.carleton.ca/about/policies/collection-profile-computer-science.

## Teaching, Learning, and Research

The information-literate student is one who is able to access information efficiently, critically assess it, assimilate and synthesize it effectively. The Library's programs and services are grounded in Ontario's Quality Assurance Framework.

The Subject Specialist works collaboratively with faculty to address students' information competencies through a number of methods, including the following.

### Instruction, Teaching, and Practicums

A total of 426 in-class instruction sessions were provided by Library staff in all subject areas during 2021-22, and a total of 10,294 students attended those sessions. This was also supplemented by over 200 videos created with over 10,000 views. The Subject Specialist designs classes and practicum opportunities to meet the needs of specific assignments and course requirements while addressing broad learning objectives.

### Learning Support – Provided Online

The Library website (library.carleton.ca) is designed to support each step of the research process: identifying, accessing, borrowing, evaluating, and citing resources. Google Analytics recorded almost 1 million visits to the Library website during 2021-22. Library users can conduct a comprehensive search of the entire collection using the Omni search interface. New improvements to Omni mean that Carleton users can now easily request to borrow items from university libraries across Canada, the United States, and other countries.

Highlights of the Library website include:

- Leading databases including: ACM Digital Library, EI Engineering Village, IEEE Xplore Digital Library, Lecture Notes in Computer Science, and O'Reilly

- Subject Guides for Computer Science & Systems and Computer Engineering

### Research Partnerships

Active research is the foundation of a strong academic program and an increasingly important part of student learning and development. The Library provides resources, services, and expertise to facilitate the Carleton research community at all levels and through all stages of the research process. This research support is provided at key service points, and through consultations and more formal collaborations.

## Services

### Individual Research Consultations

Library staff provided 3715 individual research consultations in 2021-22 for all faculties. Consultations can be scheduled for quantitative and qualitative research, as well as for GIS support.

### Research Help – Desks & CHAT

Onsite research help is provided through two service points: a Research Help desk on the main floor of the Library and a help desk in Archives and Special Collections (ASC). These two service points had a total of 5257 visits in 2019-20. Although the pandemic disrupted visits to these service points between 2020 and 2022, research help continues to be available through email and virtual platforms (over 1400 research help questions answered) and through our extended online Ask a Librarian CHAT service, which answered 2105 Carleton patron questions in 2021-22.

Results from recent user surveys show that the Library performs well in providing off-campus access to resources and services, and that these resources help people to be successful at university. The Library also does well at providing accurate answers to questions and providing course reserves that help both faculty and students.

## General Information about the Library

Carleton Library consists of five stories, totaling over 214 thousand square feet. Two floors are dedicated to silent study, while three others allow for quiet conversation. As of the Fall of 2019, the Library had a total of 2400 seats for students. This included 179 public computers and 41 bookable group study rooms. User surveys show the need for more group and silent spaces with outlets for power, and so renovations throughout the Library in the past few years continue to focus on new study space for students.

Thanks to $1 million in funding from the Government of Ontario's Training Equipment and Renewal Fund and a matching contribution from the university, the fourth floor of Carleton Library is being transformed into a newly designed space called the Future Learning Lab. This multi-purpose space can be adapted to suit a wide range of needs. It is envisioned as both a physical space and a set of programs designed to foster innovation and incentivize student-centred ways of teaching.

The New Sun Joy Maclaren Adaptive Technology Centre provides Carleton University students with disabilities, who have been referred by centrally on campus, to a pleasant comfortable place to do university work using technology adapted to their needs.

The Library's collection includes approximately 1.2 million print monographs, 2.7 million e-books, and over 260,000 e-journals in a wide range of subjects and disciplines. In addition, the

Library has substantial collections of government documents and other resources, maps, data, rare books and other special research collections, printed journals, archives, theses, multimedia resources (audio, DVD, streaming video), musical scores, as well as licensed access to full-text and indexing databases in a broad range of subjects.

Collection librarians work together with the Head of Collections & Assessment to build and maintain the Library's collection by developing collection policies that guide the systematic selection of materials. The Library also provides a request form on its website where a user may suggest a book or other item for purchase.

In order to enhance its purchasing power (particularly for electronic resources), the Library is an active member of two major cooperative partnerships: the Ontario Council of University Libraries (OCUL), a consortium of the 21 academic libraries in the province; and the Canadian Research Knowledge Network (CRKN), a consortium of 75 academic libraries across the country. Carleton Library is also a member of HathiTrust, which gives students, staff, and faculty access to a digital repository of millions of books, serials, and other materials from research institutions and libraries from around the world.

The Library's annual acquisitions budget for the 2022-2023 fiscal year is $9.1 million, and its staffing and operating budget is $14.2 million.

The Library acquisitions budget is not protected from inflation, exchange rates, or cuts, which often challenges the Library's ability to provide all the necessary resources in support of teaching, learning, and research at Carleton. Consideration of the funds necessary for the Library's acquisitions budget is part of the academic planning and Quality Assurance processes for new programs. The Library is dedicated to regular assessment of its resources and services. Staff use an assortment of qualitative and quantitative techniques to evaluate collections and services in order to make sound decisions within budget parameters.

The Library strongly supports the principles and practices of open access. The University's institutional repository, CURVE, was established in 2011 and is maintained by the Library. It includes not only a growing archive of the broad intellectual output of the University, but also digitized versions of most of the theses accepted at Carleton since 1955 – and as of 2014 houses all new Carleton theses deposited electronically. The Library contributes to CURIE, the University's program to provide funding for faculty and researchers who are publishing in open access journals, and also hosts 10 OA journals online using the Open Journal Systems management and publishing system.

# AT A GLANCE: CARLETON UNIVERSITY LIBRARY

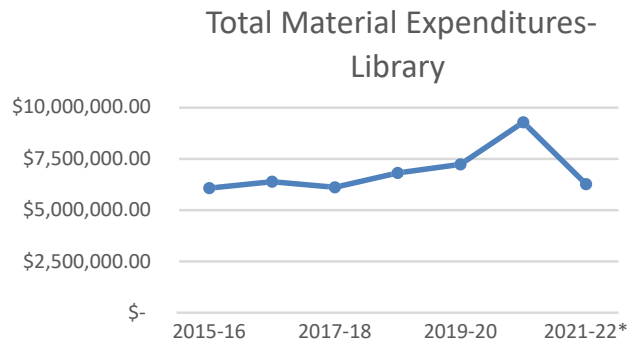
*Statistics as of May 1, 2022 except where indicated. Labour disruption*, new system implementation & effects of the pandemic** including an entire year online *** has affected some numbers*

## Research Highlights

- CURVE- Carleton's Institutional Repository
- Open Access- Funding for Faculty, Staff, & Students; Open Access Awards for Graduate Students
- Research Data Management Training

**Collection Spending:**

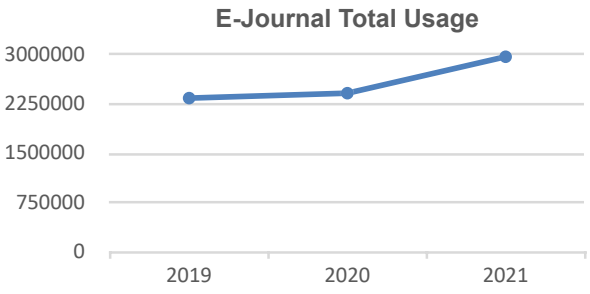
- $6.3 million; 88% of the entire collections budget spent on electronic resources
- $5.5 million spent on general electronic resources which benefit all subject areas

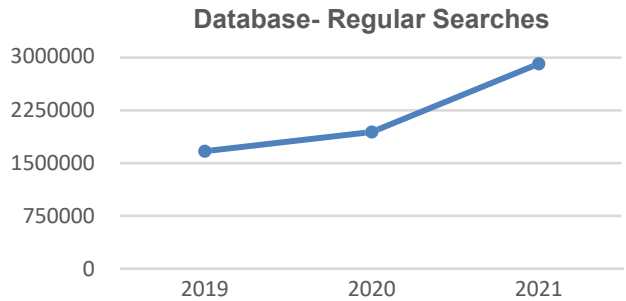


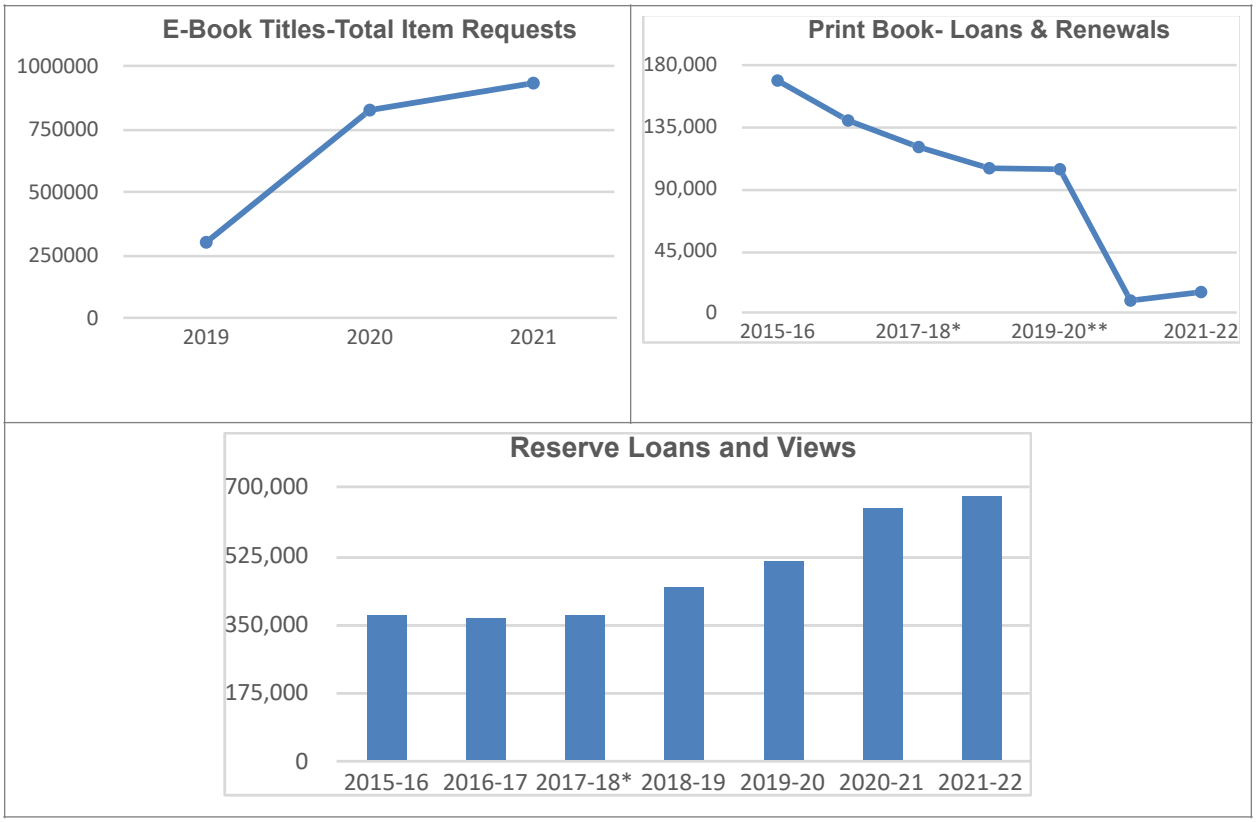

**2020-21- purchased a lot of one-time material to support the switch to online learning which did not have to be paid for again. Annual cost increases for subscriptions were lower than usual due to ongoing pandemic, & a favourable exchange rate lowered our overall spend as most of our invoices are paid in USD.*

## Collections- Usage

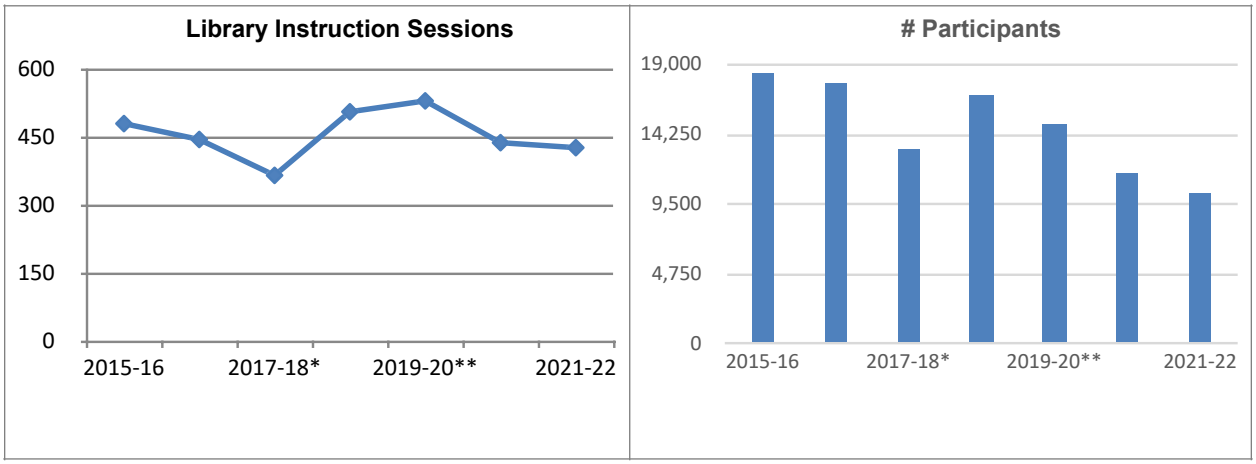
*COUNTER 5-compliant data from a selection of major e-publishers/vendors (2019 onward only)*

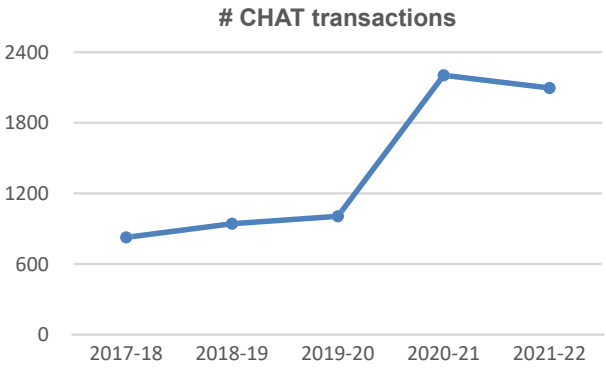





## Teaching & Learning






**Highlights for 2021-22:**

- 426 instruction sessions; 10,244 students attending
- 3715 individual research consultations in 2021-22 for all faculties
- 1400 research help questions answered (email & virtual)
- 2105 Carleton patron questions answered
- Over 200 instruction videos created with over 17,000 views

## Space

Almost 1 million visits to Library website in a year
Future Learning Lab
Adaptive Technology Centre
Innovative Study areas
Group & graduate study rooms
Book Arts Lab, an experiential learning space

# Discussant Report

New Program Review

Name: Hashmat Khan

May 15th, 2024

## Program being reviewed

Bachelor of Cybersecurity (BCSec)

## Review of self-study (Volume I)

The self-study is well-written and provides a clear description of the new Bachelor of Cybersecurity program in the School of Computer Science. There are several unique elements about this program, but the one that really stands out is the fact that it is the first program of its kind in Canada. The closest program is at the University of Ontario Institute of Technology, but that is mostly focused on 'information technology' rather than 'cybersecurity'. There are resident experts who will be involved in teaching, and the program has some unique Ottawa advantages in terms of co-op opportunities for students.

While BCSec will share a set of core courses with computer science, with an adaptation of two existing courses from the computer science security stream, there will be four new courses on security. Depending on meeting the student enrolment targets, the program will be supported by six tenure-track faculty member hires by year six.

## Review of External Reviewers' Report

The External Reviewers have made nine clear recommendations following their assessment of the program.

## Review of Unit Response and Implementation Plan

### Unit Response and Implementation Plan: Summary of Recommendations

The reviewers made nine recommendations, of which seven recommendations are '*agreed to unconditionally*' while two are '*agreed to if additional resources permit*'. Five recommendations are flagged as 'weakness', and four as 'opportunities'. Both the unit and the Dean responses adequately address these categories. The Dean's responses indicate a strong support for the recommendations and a willingness to address them in a timely manner. In particular, regarding developing a hiring plan and addressing space requirement as the program grows along the expected enrolment path.

DISCUSSANT'S CONCERN:
It was unclear from the self-study whether the BCS security stream will remain as it is now or will it be retired or folded completely into BCSec.

DISCUSSANT RECOMMENDATION:
To clarify the above point.

## Recommendation of program categorization

Recommended to commence.

**Carleton University Site Visit**
**New Undergraduate Program in Cybersecurity**
**Date: April 23, 2024**

**External Reviewers:** **Dr. David Lie,** University of Toronto
**Dr. Amr Yousseff,** Concordia University

**Internal Reviewer:** **Dr. David Mendeloff, Associate Dean, Faculty of Public Affairs**

| Time | April 23, 2024 | Location |
|---|---|---|
| 8:45 – 9:00 | Meeting with Dr. Hashmat Khan, Associate Vice-President (Academic Programs and Strategic Initiatives) | DT324 |
| 9:15 – 10:00 | Meeting with the Departmental Chair, Dr. Michel Barbeau | HP5336 |
| 10:00 – 10:30 | Department Tour with the Departmental Chair, Dr. Michel Barbeau | HP5336 |
| 10:45-11:15 | Meeting with School Administrator Mylien Reid and Undergraduate Advisor Emily Burda | HP5437 |
| 11:30 – 1:15 | LUNCH with Professors Dr. Michel Barbeau Dr. Douglas Howe & Dr. Paul Van Oorschot; and School Administrator Mylien Reid | Bakers Restaurant (Confirmed) |
| 1:30 -2:00 | Meeting with Dr. Pauline Rankin, Provost and Vice-President (Academic)<br>Dr. David Hornsby, Vice-Provost and Associate Vice-President (Academic) | 503S Tory Building |
| 2:15 – 2:45 | Meeting with Dr. Maria DeRosa, Dean, Faculty of Science | HP 3230 |
| 3:00 – 4:00 | Meeting with Faculty, Professors: Abdou, Barrera, Biddle, Chiasson, Hinek, Howe, Laurendeau, Somayaji, Stobert, Van Oorschot, & Zhao | DT303 |
| 4:15 – 4:45 | Closing Meeting with Dr. Hashmat Khan, Associate Vice-President (Academic Programs and Strategic Initiatives) | DT303 |
| 4:45 – 5:15 | External Reviewers Report Preparation Meeting | DT303 |

Please note: The meeting time slots includes travel time between offices and breaks.

**External Reviewer Biographies**
**Cybersecurity Site Visit**
**April 23, 2024**

## Dr. Amr Youssef
**Concordia University**

Dr. Amr Youssef is affiliated to Department of Computer Science & Software Engineering, Concordia University. Dr. Amr Youssef is currently providing services as Professor. Dr. Amr Youssef has authored and co-authored multiple peer-reviewed scientific papers and presented works at many national and International conferences. Dr. Amr Youssef contributions have acclaimed recognition from honourable subject experts around the world. Dr. Amr Youssef is actively associated with different societies and academies. Dr. Amr Youssef academic career is decorated with several reputed awards and funding. Dr. Amr Youssef research interests include Cryptography and network security, Sequence design for FH-CDMA, Software protection, Information hiding and Hardware implementation of cryptographic algorithms.

## Dr. David Lie
**University of Toronto**

David Lie received his BASc from the University of Toronto in 1998, and his MS and PhD from Stanford University in 2001 and 2004 respectively. He is currently a Professor in the Department of Electrical and Computer Engineering at the University of Toronto. He is known for his seminal work on the XOM architecture, which was an early precursor to modern trusted execution processor architectures such as ARM Trustzone and Intel SGX. He was the recipient of a best paper award at SOSP for this work. David is also a recipient of the MRI Early Researcher Award, Connaught Global Challenge Award and previous holder of a Canada Research Chair. He developed the PScout Android Permission mapping tool, whose datasets have been downloaded over 10,000 times and used in dozens of subsequent papers. David has served on various program committees including OSDI, Usenix Security, IEEE Security & Privacy, NDSS and CCS. Currently, his interests are focused on securing mobile platforms, cloud computing security and bridging the divide between technology and policy.

Carleton University | Office of the Vice-Provost and Associate Vice-President (Academic)

**External Reviewer Report Template – Cyclical Program Review**

The external reviewer's report serves to inform the Senate Quality Assurance and Planning Committee and Carleton University Senate. Reports can be brief on those criteria that reviewers feel are being met successfully and focus on 1) criteria that give rise to issues, on recommendations for program improvement and on 2) significant strengths, including any clearly innovative and creative aspects of the program. In the sections below you will find bullets, taken directly from the Cyclical Review Terms of Reference and Carleton University IQAP, these are items to consider and can be used as a guide but are not individual questions requiring specific responses. At the end of the document, we ask that you summarize your overall recommendations for the program.

Please note that this document will be made public, we would ask that you please refrain from using specific names or identifiers as all comments are to be held anonymous on the report.

**Recommendations**

The most important part of the report from the point of view of the university will be the recommendations made for program improvement (a minimum of 3 are required). We therefore request that all recommendations be clearly listed under 3 main categories:

- **Weakness:** Remedial action is recommended to strengthen compliance with program quality standards.
- **Concern:** Potential risk to future quality that should be considered.
- **Opportunity:** Recommendation for future enhancements

| | |
|---|---|
| **Program(s) being reviewed:** | Bachelor of Cybersecurity (BCSec) |
| **Date of review:** | April 23, 2024 |
| **Names and Emails of External Reviewers:** | Dr. David Lie (david.lie@utoronto.ca) and Dr. Amr Youssef (amr.youssef@concordia.ca) |
| **Date of Report:** | May 8, 2024 |

**Considerations for the Review**
**Note: this document list criteria for both undergraduate and graduate programs, depending on the type of review being conducted not all will need to be considered**

**Program Objectives**

- The proposed Bachelor of Cybersecurity (BCSec) perfectly aligns with Carleton University's mission and academic plans, particularly within the framework of its Strategic Integrated Plan (SIP).

1. **Alignment with SIP's Strategic Directions**: The BCSec program strongly supports two of Carleton's strategic directions: (i) "Share the knowledge, shape the future": By leveraging the research expertise of the School of Computer Science (SCS), the program aims to design a curriculum that addresses societal problems, particularly in the realm of cybersecurity. This fits within Carleton's objective of preparing students for success in an ever-changing future. (ii) "Serve Ottawa, serve the world": The program's focus on cybersecurity is highly relevant to Ottawa, given the city's significant presence of software companies and governmental organizations with interest in cybersecurity. By producing graduates equipped to address the pressing security concerns of local employers and governmental agencies, Carleton University fulfills its role in serving the Ottawa community and contributing to national security.
2. **Research Expertise and Practical Significance**: The program's emphasis on recruiting faculty members engaged in research relevant to practical cybersecurity challenges ensures that Carleton contributes meaningfully to solving real-world problems. This not only aligns with Carleton's commitment to research excellence but also enhances its reputation as a hub for addressing pressing societal issues. The program will enhance cybersecurity, an area of existing strength for Carleton University, as well as address a need in the industry.
3. **No Detrimental Impact on Existing Programs**: The BCSec program is designed in such a way that it complements rather than competes with existing academic programs at Carleton. It is specialized enough to attract a unique cohort of high-achieving students interested specifically in cybersecurity. This ensures that existing programs in Engineering, and Computer Science remain unaffected while enhancing Carleton's academic offerings.
4. **National Visibility and Attraction of Top Talent**: The uniqueness and specialization of the BCSec program position Carleton as a national leader in cybersecurity education. By attracting high-achieving students who might otherwise choose competing institutions, Carleton enhances its national visibility and reputation as an academic powerhouse in cybersecurity education.

| **Program Requirements** |
|---|

- The structure and requirements of the Bachelor of Cybersecurity (BCSec) program proposed by the School of Computer Science demonstrate a thoughtful approach to meeting its objectives and program-level learning outcomes, as well as aligning with Carleton University's Degree Level Expectations.

1. **Appropriateness of Structure and Requirements**: The program's structure, which closely mirrors the Bachelor of Computer Science (BCS) honours degree while incorporating specialized cybersecurity courses, ensures that students receive a solid foundation in core computer science principles while gaining specialized knowledge and expertise in cybersecurity. By retaining essential BCS courses and introducing new ones specific to cybersecurity, the program prepares students for security-expert roles in government and industry, as outlined in its educational goals.

2. **Alignment with Carleton's Degree Level Expectations**: The program's structure, requirements, and program-level learning outcomes are aligned with Carleton's undergraduate Degree Level Expectations. It emphasizes critical thinking, problem-solving, and communication skills essential for success in the field of cybersecurity. Moreover, by incorporating project-centered advanced courses and providing opportunities for research-related projects, the program fosters

intellectual independence and innovation, consistent with Carleton's commitment to academic excellence.

3. **Effectiveness of Mode(s) of Delivery**: The program's mode of delivery, which includes a mix of traditional classroom instruction, hands-on projects, and research opportunities, is well-suited to facilitate students' successful completion of the program-level learning outcomes. By offering a variety of learning experiences, including practical applications of security principles and exposure to current research in the field, the program ensures that students develop both theoretical knowledge and practical skills necessary for careers in cybersecurity. The combination of the program with an existing Co-op facility, such as that provided by the Shopify intern program, will enhance the skills of graduates of the program
4. **Addressing the Current State of the Discipline**: The curriculum of the BCSec program reflects the current state of the cybersecurity discipline by covering a wide range of topics, from operating systems security to human factors in security. By incorporating both foundational concepts and emerging trends in cybersecurity, such as cloud security and blockchain applications, the program equips students with relevant knowledge and skills needed to address contemporary security challenges.
5. **Program Innovations and High-Impact Practices**: The BCSec program introduces several innovative components, including project-centered advanced courses, research-related projects, and electives that allow students to explore specialized areas within cybersecurity. By offering flexibility in course selection and providing opportunities for hands-on learning and research collaboration, the program enhances the educational experience and prepares students for leadership roles in the field of cybersecurity.

## Program Requirements for graduate programs only

N/A

## Assessment of Teaching and Learning

- The assessment plan outlined for the Bachelor of Cybersecurity (BCSec) program demonstrates a comprehensive approach to evaluating student achievement of program-level learning outcomes and degree level expectations, as well as ensuring the overall quality and effectiveness of the program.

1. **Assessment Methods**: The utilization of course outline and material repositories, along with a database of student marks, provides robust sources of evidence for assessing student achievement of learning outcomes. By collecting data on course materials, assignments, exams, and student projects, the curriculum committee can effectively evaluate the extent to which students are mastering the intended knowledge and skills outlined in the program's learning outcomes.
2. **Monitoring and Assessment Plans**: The planned timeline for conducting assessments, spanning multiple years and focusing on different sets of learning outcomes each year, allows for a systematic and thorough evaluation of the program's effectiveness. By assessing learning

outcomes at regular intervals and across various stages of the program, the curriculum committee can monitor whether the program is achieving its objectives and whether students are successfully meeting the desired outcomes.

3. **Continuous Improvement**: The involvement of the School Council and the curriculum committee in reviewing assessment results and implementing recommendations ensures a collaborative approach to program improvement. By disseminating assessment findings and discussing them at regular meetings, faculty members and student representatives can contribute to informed decision-making aimed at enhancing the overall quality of the program.
4. **Accommodations for Accessibility**: The program's recognition of essential requirements and accommodations aligns with principles of equity and inclusivity in education. By ensuring that accommodations do not compromise the standards or outcomes of the program, but rather provide equal opportunities for all students to succeed, the BCSec program promotes an environment conducive to learning and growth for students with diverse needs.

## Admission Requirements

- The admissions requirements outlined for the Bachelor of Cybersecurity (BCSec) program reflect a thoughtful consideration of the program's objectives and program-level learning outcomes, ensuring that admitted students are well-prepared to succeed in the program.

1. **Alignment with Program Objectives**: By raising the minimum entrance average and requiring both Calculus and Vectors and Advanced Functions, the admissions requirements for the BCSec program are designed to attract high-achieving students who possess strong foundational knowledge in mathematics and computing. This aligns with the program's objectives of preparing students for security-expert roles in government and industry by ensuring that admitted students have the academic aptitude and background necessary to excel in the program.
2. **Competitive Positioning**: The decision to raise the minimum entrance average, in part to align with competitors like Waterloo, demonstrates a strategic approach to positioning the BCSec program within the academic landscape. By setting a higher entrance standard, the program signals its commitment to excellence and distinguishes itself as a rigorous and prestigious option for prospective students interested in cybersecurity education.
3. **Recognition of Prior Learning**: While the admissions requirements primarily focus on academic achievement in high school, they also indirectly recognize the importance of prior learning and experience in mathematics and computing. By requiring specific math courses and setting a higher entrance average, the program acknowledges the value of foundational knowledge and skills acquired through previous coursework or extracurricular activities.

## Resources

- The resources outlined for the Bachelor of Cybersecurity (BCSec) program demonstrate a robust infrastructure to support the program's goals and foster an enriching academic environment for students.

1. **Qualified Core Faculty**: The School of Computer Science boasts a team of dedicated support and technical staff, including Undergraduate Program Advisors, Technical Staff, and Lab Coordinators, who play integral roles in supporting the delivery of the program. With their

expertise in advising students, managing computing infrastructure, and overseeing tutorial/lab components, these staff members contribute to the overall success of the program and ensure students receive adequate support throughout their academic journey.

2. **Utilization of Adjunct and Part-Time Faculty**: While the program primarily relies on core faculty and staff members, the inclusion of adjunct and part-time faculty can further enrich the academic experience by bringing industry expertise and diverse perspectives to the classroom. The program's emphasis on sustainability includes plans to ensure the quality of adjunct and part-time faculty appointments, thereby maintaining the integrity and effectiveness of the program delivery.
3. **Supervision of Experiential Learning Opportunities**: The presence of Lab Coordinators who manage the tutorial/lab components of courses ensures that students have access to hands-on experiential learning opportunities. These coordinators play a crucial role in overseeing lab exercises, providing training and supervision to teaching assistants, and assessing the effectiveness of laboratory exercises, thereby enhancing the practical learning experiences of students.
4. **Utilization of Existing Resources**: The program leverages existing human, physical, and financial resources effectively to support its delivery. With dedicated technical staff responsible for managing computing infrastructure, classroom spaces equipped with necessary technology, and collaboration spaces available across the university campus, the program maximizes the use of existing resources to meet its needs.
5. **Library Support and Information Technology**: The Carleton University Library provides essential resources to support the BCSec program, including access to electronic subscriptions covering major publication venues in computer science and security. The library's collection is tailored to support the program's curriculum, ensuring that students have access to relevant research materials and information resources to support their scholarly activities. Additionally, the program makes extensive use of information technology resources, such as cloud computing and virtualization environments, managed by dedicated technical staff, further enhancing the quality of scholarship and research activities produced by students.

## Resources for graduate programs only

N/A

## Quality and other indicators

- The information provided regarding the core faculty of the Bachelor of Cybersecurity (BCSec) program demonstrates a high level of expertise, commitment to teaching, and potential for student mentorship, ensuring the intellectual quality of the student experience.

1. **Faculty Qualifications and Expertise**: From the information supplied about the core faculty members, it is evident that they possess diverse areas of specialization in cybersecurity, including Internet security, network security, human-computer interaction, software security, and cryptography. Their ranks range from Assistant Professors to Full Professors, indicating a mix of early-career researchers and seasoned academics with extensive experience.
2. **Research Funding and Scholarly Record**: The faculty's track record of securing research funding from various sources, including federal government agencies, industry partners, and internal grants, underscores their scholarly achievements and the relevance of their research to real-

world applications. The substantial amount of funding obtained over the years reflects the quality and impact of their research endeavors.

3. **Teaching Assignments and Commitment to Student Mentoring**: The recent teaching assignments of core faculty members demonstrate their dedication to undergraduate and graduate education within the School of Computer Science (SCS). The supplied information also highlights the faculty members' commitment to student learning and mentorship. Additionally, the provision for hiring additional teaching-track faculty and contract instructors underscores the program's commitment to maintaining high teaching standards and ensuring adequate support for student learning.
4. **Scholarly Output and Student Success**: While the program does not require a thesis or capstone project, students will engage in substantial projects in advanced security courses, providing them with practical experience and opportunities for scholarly output. Furthermore, the faculty's involvement in provincial and national scholarships, competitions, and awards reflects their commitment to fostering student success and providing opportunities for professional development.

**Additional Comments:**

Overall, the Bachelor of Cybersecurity (BCSec) program proposed by the School of Computer Science at Carleton University demonstrates a strong alignment with the university's strategic objectives, academic mission, and commitment to excellence in education and research. The program's innovative curriculum, emphasis on practical learning, and comprehensive assessment plan ensure the intellectual quality of the student experience and prepare graduates for success in the rapidly evolving field of cybersecurity. Given the program's significant strengths, including its alignment with Carleton's Strategic Integrated Plan, research expertise, effective utilization of resources, and commitment to student success and mentorship, I recommend that Carleton University proceed with the implementation of the Bachelor of Cybersecurity program. This program has the potential to enhance Carleton's reputation as a leader in cybersecurity education, attract top talent, and contribute to the academic and professional development of future cybersecurity professionals. Note that in the recommendations below, we have considered "Concerns" the most severe, "Weakness" less severe and "Opportunity" as the least severe.

**Summary of Recommendations/Program Enhancements**

Use the chart below to summarize your overall recommendations for the program and suggested program enhancements.

| **Recommendation** | **Category** *(Weakness, Concern, Opportunity)* |
|---|---|
| 1) Based on the vital role played by the Undergraduate Program Advisors in supporting the undergraduate programs offered by the School of Computer Science (SCS), including the | Weakness |

| | |
|---|---|
| proposed Bachelor of Cybersecurity (BCSec) program, it is strongly recommend converting the temporary position into a permanent one. The Undergraduate Program Advisors are instrumental in providing essential administrative support, advising students on program requirements, facilitating program adjustments for transfer students, and ensuring the smooth progression of students through their academic journey. In addition, to address the challenges faced by the advising desk in terms of privacy and accessibility, it is recommended to establish a third advising office dedicated specifically to in-person advising (currently, the third non-permanent advisor is assigned a “floating” desk). | |
| 2) Table B.2 illustrates the alignment of each BCSec learning outcome with the corresponding Degree Level Expectations (DLEs) it contributes to. A brief explanation of the rationale behind this mapping should be provided. | Weakness |
| 3) Given the specialized nature of many of the security courses, hiring qualified TAs might pose a challenge. Since graduate students in the security group constitute the primary pool for these TA positions, allocating TAships to these graduate students can help alleviate this issue. Also providing special entrance awards and scholarships for graduate students in this area can help attract graduate students to the security group who can eventually also serve as TAs for the proposed program. | Weakness |
| 4) While the program is transitioning to a Bring Your Own Device (BYOD) model for students, it's imperative to acknowledge the ongoing need for IT support to address potential issues arising from students' personal devices, such as compatibility, software licensing and technical problems. Additionally, students should be well-informed about the minimum specifications required for their devices and any potential restrictions associated with them. Possible (financial) equity issues related to BYOD can be addressed/mitigated through bursaries. | Weakness |
| 5) Ensuring the successful recruitment of the six new faculty members may pose challenges due to factors such as competition in the academic job market and the specific expertise required for the program. Therefore, it is advisable to initiate | Weakness |

| | |
|---|---|
| the hiring cycle well in advance to allow sufficient time for advertising positions, conducting thorough searches, and selecting the most qualified candidates. It is also recommended to allocate office and lab space for these newly hired faculty members within the same vicinity as the existing security group. This arrangement fosters coherence and facilitates collaboration among faculty members, promoting a seamless exchange of ideas and expertise. | |
| 6) The description of the courses reveal that "ethics" is only explicitly addressed in COMP 2109: "Introduction to Security and Privacy," with no direct reference in the remaining listed courses. To address this concern in the Bachelor of Cybersecurity (BCSec) program's course descriptions, it is recommended to conduct a curriculum review involving faculty with expertise in cybersecurity ethics. This review should identify opportunities to integrate ethics-related content into courses beyond COMP 2109. Other topics such as AI security/privacy and the use of AI for security may also be considered. | Opportunity |
| 7) Given that certain co-op opportunities for students in this program may necessitate a security clearance, a process that can be time-consuming, it is recommended that students initiate this procedure at least 12 to 18 months prior to their intended placement. | Opportunity |
| 8) Clarify and identify any potential overlap between courses to ensure coherence and consistency across the curriculum. | Opportunity |
| 9) Incorporating Equity, Diversity, and Inclusion (EDI) principles into the program curriculum is essential to fostering a supportive and inclusive learning environment. By integrating EDI components into course content, assignments, and discussions, the program can promote awareness and understanding of diverse perspectives and experiences within the field of cybersecurity. Moreover, allocating scholarship awards specifically for EDI support (e.g., scholarships dedicated for Indigenous people) can further encourage diversity and inclusion within the student body, providing opportunities for underrepresented groups to excel in the program. | Opportunity |

**Cybersecurity**
**Unit Response to External Reviewers' Report & Implementation Plan**
**Programs Being Reviewed: Undergraduate Programs**

## Note: This document is forwarded to Senate, the Quality Council and posted on the Vice- Provost's external website.

**Introduction & General Comments**

The School of Computer Science was pleased to receive the Reviewers' very positive External Reviewers' Report on May 9, 2024 This report was shared with our faculty and staff, and we are committed to the continual improvement of our programs to enhance the student, staff, and faculty experience. This document contains both a response to the External Reviewers' Report and an Implementation Plan (Section B), which have been created in consultation with Dr. Maria DeRosa, the Dean of the Faculty of Science.

For each recommendation one of the following responses must be selected:

**Agreed to unconditionally:** used when the unit agrees to and is able to take action on the recommendation without further consultation with any other parties internal or external to the unit.
**Agree**d to **if additional resources permit:** used when the unit agrees with the recommendation, however action can only be taken if additional resources are made available. Units must describe the resources needed to implement the recommendation and provide an explanation demonstrating how they plan to obtain those resources. In these cases, discussions with the Deans will normally be required and therefore identified as an action item.
**Agreed to in principle:** used when the unit agrees with the recommendation, however action is dependent on something other than resources. Units must describe these dependencies and determine what actions, if any, will be taken.
**Not agreed to:** used when the unit does not agree with the recommendation and therefore will not be taking further action. A rationale must be provided to indicate why the unit does not agree (no action should be associated with this response).

**Calendar Changes**

If any of the action items you intend to implement will result in calendar changes, please describe what those changes will be. To submit a formal calendar change, please do so using the Courseleaf system.

| UNIT RESPONSE AND IMPLEMENTATION PLAN<br>Programs Being Reviewed: Cybersecurity<br>Prepared by (name/position/unit/date): Doug Howe, Professor, School of Computer Science, May 13, 2024 | | | | | |
|---|---|---|---|---|---|
| **External Reviewer Recommendation & Categorization** | **Unit Response:**<br>**1- Agreed to unconditionally**<br>**2- Agreed to if additional resources permit (describe resources)**<br>**3- Agreed to in principle**<br>**4- Not agreed to**<br>**Rationales are required for categories 2, 3 & 4** | **Action Item** | **Owner** | **Timeline** | **Will the action described require calendar changes? (Y or N)** |
| 1) **Weakness**- Based on the vital role played by the Undergraduate Program Advisors in supporting the undergraduate programs offered by the School of Computer Science (SCS), including the proposed Bachelor of Cybersecurity (BCSec) program, it is strongly recommend converting the temporary position into a permanent one. The Undergraduate Program Advisors are instrumental in providing essential administrative support, advising students on program requirements, facilitating program adjustments for transfer students, and ensuring the smooth progression of students through their academic journey. In addition, to address the challenges faced by the advising desk in terms of privacy and accessibility, it is recommended to establish a third advising office dedicated specifically to in-person advising (currently, the third non-permanent advisor is assigned a “floating” desk). | **Agreed to if additional resources permit.** | Initially, the program will not be admitting students into upper years. The total enrolment will start small and ramp up over the next three years. We agree on the importance of undergraduate advising and intend to implement this recommendation if justified by the eventual enrolment.<br><br>The SCS Director will revisit the administrative need of the Cybersecurity program after the program has started and when we have firm enrolment projections and make recommendations to the Dean of the Faculty of Science.<br><br>The Dean of the Faculty of Science will advocate for additional resources as necessary during the yearly budget cycle. | Director, School of Computer Science | Discussions will occur starting September 2025 and, if needed, September 2026. | N |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| 2) **Weakness-**Table B.2 illustrates the alignment of each BCSec learning outcome with the corresponding Degree Level Expectations (DLEs) it contributes to. A brief explanation of the rationale behind this mapping should be provided. | **Agreed to unconditionally.** | Update Table B.2 as recommended. | Program Lead, Cybersecurity | May 2024 | N |
| 3) **Weakness-**Given the specialized nature of many of the security courses, hiring qualified TAs might pose a challenge. Since graduate students in the security group constitute the primary pool for these TA positions, allocating TAships to these graduate students can help alleviate this issue. Also providing special entrance awards and scholarships for graduate students in this area can help attract graduate students to the security group who can eventually also serve as TAs for the proposed program. | **Agreed to unconditionally.** | No change required. TAships will continue to be available for essentially all grad students coming to Carleton for graduate work in CS. We will have an increase in RAships, TAships, and scholarships, as students are eligible, due to the increased number of faculty in this field. | N/A | N/A | N |
| 4) **Weakness-**While the program is transitioning to a Bring Your Own Device (BYOD) model for students, it's imperative to acknowledge the ongoing need for IT support to address potential issues arising from students' personal devices, such as compatibility, software licensing and technical problems. Additionally, students | **Agreed to unconditionally.** | 1. Update BYOD hardware requirements for BCSec students as needed.<br><br>2. Ensure SCS IT staff can provide BCSec-specific tech support. | Director, School of Computer Science<br><br>Associate Dean, Equity, | Discussions will start September 2024 | N |

| | | | | | |
|---|---|---|---|---|---|
| should be well-informed about the minimum specifications required for their devices and any potential restrictions associated with them. Possible (financial) equity issues related to BYOD can be addressed/mitigated through bursaries. | | 3. Software needed for Computer Science programs are offered for free or discounted to students. Currently, there are a few initiatives being trialed to increase hardware access for students. Students have access to Virtual Desktop infrastructure through SCS. There may also be computers made available from updating computer tutorial classrooms. The MacOdrum Library has loaner laptops available, and ITS has computer labs available to Carleton students. The School of Computer Science will continue to discuss equity issues with appropriate Carleton staff and ensure the BYOD policy can address and mitigate these issues. | Diversity, and Inclusion, Faculty of Science | | |
| 5) **Weakness-**Ensuring the successful recruitment of the six new faculty members may pose challenges due to factors such as competition in the academic job market and the specific expertise required for the program. Therefore, it is advisable to initiate the hiring cycle well in advance to allow sufficient time for advertising positions, conducting thorough searches, and selecting the most qualified candidates. It is also recommended to allocate office and lab space for these newly hired faculty members within the same vicinity as the existing security group. This arrangement fosters coherence and facilitates collaboration among faculty | **Agreed to if additional resources permit.** | We will plan modifications to our hiring process that address the current high demand for security faculty, e.g., advertise earlier in the year, advertise in an expanded set of mail lists, web sites and publications, and strongly encourage current faculty to exploit their own networks. We will approach the Dean of Science as necessary during the budget allocation process.<br><br>We will implement recommendations as part of general plan to expand SCS office and lab space. | Director, School of Computer Science | We will complete a hiring plan in the 2024/5 academic year.<br><br>We will begin discussions on office space in Fall 2024. | N |

| | | | | | |
|---|---|---|---|---|---|
| members, promoting a seamless exchange of ideas and expertise. | | | | | |
| 6) **Opportunity-**The description of the courses reveal that "ethics" is only explicitly addressed in COMP 2109: "Introduction to Security and Privacy," with no direct reference in the remaining listed courses. To address this concern in the Bachelor of Cybersecurity (BCSec) program's course descriptions, it is recommended to conduct a curriculum review involving faculty with expertise in cybersecurity ethics. This review should identify opportunities to integrate ethics-related content into courses beyond COMP 2109. Other topics such as AI security/privacy and the use of AI for security may also be considered. | **Agreed to unconditionally.** | Will review and incorporate ethics into appropriate core security courses. | Director, Bachelor of Cybersecurity | Review will start before October 2024. | Y |
| 7) **Opportunity-**Given that certain co-op opportunities for students in this program may necessitate a security clearance, a process that can be time-consuming, it is recommended that students initiate this procedure at least 12 to 18 months prior to their intended placement. | **Agreed to unconditionally.** | In consultation with federal government security employers (e.g., CSE and DND), create advising plan to ensure students apply early for security clearance appropriate to BCSec co-op positions in government. | Director, Bachelor of Cyber Security | Will reach out to necessary stakeholders by December 2024. | N |

| | | | | | |
|---|---|---|---|---|---|
| 8) **Opportunity-**Clarify and identify any potential overlap between courses to ensure coherence and consistency across the curriculum. | **Agreed to unconditionally.** | Give special attention to overlap when elaborating the curriculum. | Director, Bachelor of Cyber Security | Review will start before October 2024. | N |
| 9) **Opportunity-**Incorporating Equity, Diversity, and Inclusion (EDI) principles into the program curriculum is essential to fostering a supportive and inclusive learning environment. By integrating EDI components into course content, assignments, and discussions, the program can promote awareness and understanding of diverse perspectives and experiences within the field of cybersecurity. Moreover, allocating scholarship awards specifically for EDI support (e.g., scholarships dedicated for Indigenous people) can further encourage diversity and inclusion within the student body, providing opportunities for underrepresented groups to excel in the program. | **Agreed to unconditionally.** | The Faculty of Science is committed to incorporating Equity, Diversity, and Inclusion (EDI) principles into teaching and learning at Carleton. Lecturers and Professors are encouraged to complete the Kinàmàgawin Indigenous Learning Certificate and the Department of Equity and Inclusive Communities' "Equity and Human Rights", "Equity in Your (work) Space – Faculty, Staff and Supervisors", "Inclusive Classroom – Faculty", "Responding to Disclosures of Sexual Violence", and "Breaking Down Barriers: Exploring Disability, Dignity and Ableism" modules. Furthermore, the Faculty promotes its EDI Teaching Toolkit, and Research Pocket Guide.<br><br>Currently, students in the Faculty of Science can apply for the Black and Indigenous Summer Research Internship (BISRI) which grants student a paid summer research internship on a topic of their choice. This program is available to Bachelor of Cybersecurity students. | Director, Bachelor of Cyber Security<br><br>Associate Dean, Equity, Diversity, and Inclusion, Faculty of Science | Exploring how to best incorporate EDI into program curriculum will occur before December 2024. | N |

**Cybersecurity**
**Dean's Response**
**Programs Being Reviewed: Bachelor of Cybersecurity**
**Date: May 14th 2024**
**Version: 1**

**Instruction**
The table below has been pre-populated with the external reviewer recommendations. Please complete the Dean's Response column by providing a separate response to each of the external reviewers' recommendations, as required by the QAF (5.3.1).

| **Dean's Response**<br>**Programs Being Reviewed: Bachelor of Cybersecurity**<br>**Prepared by: Maria DeRosa** | | |
|---|---|---|
| **External Reviewer Recommendation & Categorization** | **Dean's response**<br>**A response is required for each recommendation listed.** | |
| **1. Weakness**- Based on the vital role played by the Undergraduate Program Advisors in supporting the undergraduate programs offered by the School of Computer Science (SCS), including the proposed Bachelor of Cybersecurity (BCSec) program, it is strongly recommend converting the temporary position into a permanent one. The Undergraduate Program Advisors are instrumental in providing essential administrative support, advising students on program requirements, facilitating program adjustments for transfer students, and ensuring the smooth progression of students through their academic journey. In addition, to address the challenges faced by the advising desk in terms of privacy and accessibility, it is recommended to establish a third advising office dedicated specifically to in-person advising (currently, the third non-permanent advisor is assigned a "floating" desk). | I am in full agreement that advising is a critical part of the student experience. The Office of the Dean of Science will provide bridging administrative support for all new programs, including Cybersecurity. I agree to advocate for resources for Cybersecurity through the yearly budget allocation process concomitant with the program reaching its expected and reasonable enrollment targets. It is also important to note that the Faculty level supports such as the Science Student Success Centre and central supports such as the Academic Advising Centre will be available to all Cybersecurity students in addition to the School level supports. | |

| | |
|---|---|
| **2. Weakness-**Table B.2 illustrates the alignment of each BCSec learning outcome with the corresponding Degree Level Expectations (DLEs) it contributes to. A brief explanation of the rationale behind this mapping should be provided. | I see that this has been completed by the unit and I support this amendment. |
| **3. Weakness-**Given the specialized nature of many of the security courses, hiring qualified TAs might pose a challenge. Since graduate students in the security group constitute the primary pool for these TA positions, allocating TAships to these graduate students can help alleviate this issue. Also providing special entrance awards and scholarships for graduate students in this area can help attract graduate students to the security group who can eventually also serve as TAs for the proposed program.<br>1. | Priority TAships are distributed by the Faculty and I fully support that we will provide qualified TAs for this program from that allotment. |
| **4. Weakness-**While the program is transitioning to a Bring Your Own Device (BYOD) model for students, it's imperative to acknowledge the ongoing need for IT support to address potential issues arising from students' personal devices, such as compatibility, software licensing and technical problems. Additionally, students should be well-informed about the minimum specifications required for their devices and any potential restrictions associated with them. Possible (financial) equity issues related to BYOD can be addressed/mitigated through bursaries. | Equity is a key priority for the Faculty of Science and I am supportive of the initiatives outlined in the unit response to help mitigate any financial barriers. I am tasking our Associate Dean, Equity, Diversity, and Inclusion, Faculty of Science to be part of these conversations moving forward and to assess the need for additional supports. |
| **5. Weakness-**Ensuring the successful recruitment of the six new faculty members may pose challenges due to factors such as competition in the academic job market and the specific expertise required for the program. Therefore, it is advisable to initiate the hiring cycle well in advance to allow sufficient time for advertising positions, conducting thorough searches, and selecting the most qualified candidates. It is also recommended to allocate office and lab space for these newly hired faculty members within the same vicinity as the existing security group. This arrangement fosters coherence and facilitates collaboration among faculty members, promoting a seamless exchange of ideas and expertise. | Recognizing the recruiting challenge as described, we will support the unit as they follow their hiring plan as the specified enrolment targets are met. As the program grows towards its projected targets, I recognize that additional faculty space will be needed. The Faculty of Science is developing a cohesive plan to address space issues across the Faculty. The space needs of new programs such as Cybersecurity will be considered and prioritized within this plan, in consultation with the unit's space committee. I will continue to advocate for space on an ongoing basis and allocate it appropriately as Cybersecurity reaches its enrolment targets. |
| **6. Opportunity-**The description of the courses reveal that "ethics" is only explicitly addressed in COMP 2109: "Introduction to Security and | Ensuring that programs contain relevant and important material is a part of the curriculum committee's role both at a Faculty and central level. I fully support this opportunity as it aligns directly with an action in our |

| | |
|---|---|
| Privacy," with no direct reference in the remaining listed courses. To address this concern in the Bachelor of Cybersecurity (BCSec) program's course descriptions, it is recommended to conduct a curriculum review involving faculty with expertise in cybersecurity ethics. This review should identify opportunities to integrate ethics-related content into courses beyond COMP 2109. Other topics such as AI security/privacy and the use of AI for security may also be considered. | strategic plan: “To prepare students for success in an everchanging future, we will: Train students to use disruptive technologies productively and ethically.” |
| **7. Opportunity-**Given that certain co-op opportunities for students in this program may necessitate a security clearance, a process that can be time-consuming, it is recommended that students initiate this procedure at least 12 to 18 months prior to their intended placement. | I support the plan to make the security clearance process more efficient and have clear communications to students. |
| **8 .Opportunity-**Clarify and identify any potential overlap between courses to ensure coherence and consistency across the curriculum. | I am fully supportive of this recommendation as this is an important, routine part of the curriculum committee’s role and IQAP process. |
| **9. Opportunity-**Incorporating Equity, Diversity, and Inclusion (EDI) principles into the program curriculum is essential to fostering a supportive and inclusive learning environment. By integrating EDI components into course content, assignments, and discussions, the program can promote awareness and understanding of diverse perspectives and experiences within the field of cybersecurity. Moreover, allocating scholarship awards specifically for EDI support (e.g., scholarships dedicated for Indigenous people) can further encourage diversity and inclusion within the student body, providing opportunities for underrepresented groups to excel in the program. | Incorporating EDI principles in all of Science, including Cybersecurity is a key goal of the Faculty of Science, and an important part of our strategic plan. I support this recommendation whole-heartedly. Our Associate Dean of EDI has struck a committee made up of reps from all programs, and would welcome a rep from Cybersecurity. Our faculty have access to training to support them in their roles such as the Kinàmàgawin Indigenous Learning Certificate, modules from the Department of Equity and Inclusive Communities’ “such as “Inclusive Classroom – Faculty”. Each program also has a teaching mentor who takes their inclusive teaching practices back to the unit. Furthermore, we promote the use of our EDI Teaching Toolkit (https://science.carleton.ca/toolkit/), and Research Pocket Guide (https://science.carleton.ca/about/edi/pocketguide/). Undergraduate students in the Faculty of Science can apply for the Black and Indigenous Summer Research Internship (BISRI) which grants student a paid summer research internship on a topic of their choice. This program will be available to Bachelor of Cybersecurity students. |

**Date:** May 23, 2024

**To:** Dr. Michel Barbeau, Director, School of Computer Science
Dr. Douglas Howe, Professor, School of Computer Science

**From:** Dr. David Hornsby, Vice-Provost and Associate Vice-President (Academic);
Chair, Senate Quality Assurance and Planning Committee

**Cc:** Dr. Maria DeRosa, Dean, Faculty of Science
Dr. Julia Wallace, Associate Dean (Undergraduate Affairs), Faculty of Science
Dr. Hashmat Khan, Associate Vice-President (Academics Programs and Strategic Initiatives)
Christina Noja, Director, Office of Academics Programs and Strategic Initiatives
Dr. Robyn Green, Program Officer, Office of Academics Programs and Strategic Initiatives
Dr. Lizzie Yan, Program Assessment Specialist, Office of Academics Programs and Strategic Initiatives

**RE: Outcome of New Program Proposal**

---

The Senate Quality Assurance and Planning Committee (SQAPC) met on **May 23, 2024,** to consider the unit's response to the External Reviewers' report for the following new program proposal:

- **Bachelor of Cybersecurity**

In accordance with article 3.5.8 of Carleton's Institutional Quality Assurance Process, SQAPC has determined the outcome of the programs as "**Recommended to commence**".

The committee did however make the following requests:

1) That the unit remove the "Supervision privileges" column in table D1, they felt this information was not required as part of an undergraduate program.
2) An interim report on the unit response be submitted by January 30, 2025. To report specifically on the action relating to recommendation #9. On this topic the committee also recommended that EDI be included in course calendar language.

In addition to the recommendations made by the committee, our office has reviewed the additions to table B2, and would like to recommend that rationales for LOs 1, 4 and 9 be added for consistency.

**Office of the Vice-Provost & Associate Vice-President (Academic)**

4th Floor, Dunton Tower
1125 Colonel By Drive
Ottawa, ON K1S 5B6 Canada

**T** (613) 520-4027
david.hornsby@carleton.ca
www.carleton.ca/viceprovost

If you could please forward your responses as an updated Volume to Christina Noja by Tuesday May 28, 2024. The file will then be updated and forwarded to Senate for consideration.

Please do not hesitate to contact me should you have any questions or concerns.

Sincerely,

Professor David J Hornsby, BA (Hons), MA, PhD (Cantab)
Vice-Provost and Associate Vice-President (Academic)
Professor of International Affairs

**Office of the Vice-Provost & Associate Vice-President (Academic)**

4th Floor, Dunton Tower
1125 Colonel By Drive
Ottawa, ON K1S 5B6 Canada

**T** (613) 520-4027
david.hornsby@carleton.ca
www.carleton.ca/viceprovost

Carleton University | Faculty of Science

FACULTY OF SCIENCE
3230 HERZBERG LABORATORIES
CARLETON UNIVERSITY
1125 COLONEL BY DRIVE
OTTAWA, ONTARIO, K1S 5B6

May 21, 2024

**Re: Letter of Support for the Bachelor of Cybersecurity**

To whom it may concern,

I am delighted to offer my enthusiastic support for the proposed Bachelor of Cybersecurity. The cybersecurity landscape is evolving at an unprecedented pace, and the demand for qualified individuals to protect sensitive information and maintain secure systems has never been greater. A dedicated undergraduate program in cybersecurity at Carleton University would not only help fill the projected talent gap but also position the university as a leader in this vital field.

The Faculty of Science at Carleton is uniquely positioned to offer a rigorous cybersecurity program that combines theoretical knowledge with practical application. The proposed new degree in cybersecurity builds on the well-established and successful Bachelor of Computer Science (BCS) honours program by incorporating its robust core curriculum, adapting the foundational security courses from the BCS Security Stream, and introducing six innovative courses specifically focused on advanced security topics. The program will be produce professionals who understand how to design, build, and analyze secure software and systems, and who have sufficient fundamental knowledge to enable them not only to react to changes in the security landscape but to anticipate them. The proposed program has received strong support from the entire university and all relevant units. This initiative aligns with the pressing needs of our society and Carleton's strategic goals. I am confident that the program will produce highly skilled graduates who will make substantial contributions to the cybersecurity industry and beyond. I therefore strongly support the launch of this new program.

Sincerely,

Maria DeRosa, Ph.D.
Dean, Faculty of Science
Carleton University

# New Program Proposal

Date Submitted: 04/04/24 1:14 pm

## Viewing: TBD-2258 : Cybersecurity B.Cyber. Honours

Last edit: 05/28/24 10:46 am

Last modified by: nataliephelan

Changes proposed by: michelbarbeau

### In Workflow

1. **COMP ChairDir UG**
2. **SCI Dean**
3. **COMP FCC**
4. **COMP FBoard**
5. **PRE SCCASP**
6. **SCCASP**
7. **SQAPC**
8. Senate
9. PRE CalEditor
10. CalEditor

### Approval Path

1. 04/04/24 1:15 pm Michel Barbeau (michelbarbeau): Approved for COMP ChairDir UG
2. 04/10/24 11:59 am Julia Wallace (juliawallace): Approved for SCI Dean
3. 04/10/24 12:06 pm Michel Barbeau (michelbarbeau): Approved for COMP FCC
4. 04/10/24 12:15 pm Michel Barbeau (michelbarbeau): Approved for COMP FBoard
5. 05/21/24 11:24 am Natalie Phelan (nataliephelan): Approved for PRE SCCASP
6. 05/28/24 12:29 pm Erika Strathearn (erikastrathearn): Approved for SCCASP

| | |
|---|---|
| Effective Date | 2025-26 |
| Workflow | majormod |
| Program Code | TBD-2258 |

| | |
|---|---|
| Level | Undergraduate |
| Faculty | Faculty of Science |
| Academic Unit | School of Computer Science |
| Degree | |
| Title | Cybersecurity B.Cyber. Honours |

## Program Requirements

---

## Cybersecurity
## B.Cyber. Honours (20.0 credits)

A. Credits Included in the Major CGPA (11.5 credits)

| | | | |
|---|---|---|---|
| **1. 5.0 credits in:** | | | 5.0 |
| COMP 1405 | [0.5] | Introduction to Computer Science I | |
| COMP 1406 | [0.5] | Introduction to Computer Science II | |
| COMP 1805 | [0.5] | Discrete Structures I | |
| COMP 2401 | [0.5] | Introduction to Systems Programming | |
| COMP 2402 | [0.5] | Abstract Data Types and Algorithms | |
| COMP 2404 | [0.5] | Introduction to Software Engineering | |
| COMP 2406 | [0.5] | Fundamentals of Web Applications | |
| COMP 2804 | [0.5] | Discrete Structures II | |
| COMP 3000 | [0.5] | Operating Systems | |
| COMP 3004 | [0.5] | Object-Oriented Software Engineering | |
| **2. 2.5 credits in:** | | | 2.5 |
| COMP 2109 | [0.5] | Introduction to Security and Privacy | |
| COMP 3008 | [0.5] | Human-Computer Interaction | |
| COMP 3203 | [0.5] | Principles of Computer Networks | |
| CSEC 2108 | [0.0] | Course CSEC 2108 Not Found | |
| CSEC 3108 | [0.0] | Course CSEC 3108 Not Found | |
| **3. 1.0 credit from:** | | | 1.0 |
| COMP 3002 | [0.5] | Compiler Construction | |
| COMP 3301 | [0.5] | Technical Writing for Computer Science | |
| COMP 4004 | [0.5] | Software Quality Assurance | |
| COMP 4203 | [0.5] | Wireless Networks and Security | |
| MATH 2108 | [0.5] | Abstract Algebra I | |
| **4. 3.0 credits in:** | | | 3.0 |
| CSEC 4000 | [0.0] | Course CSEC 4000 Not Found | |
| CSEC 4100 | [0.0] | Course CSEC 4100 Not Found | |
| CSEC 4200 | [0.0] | Course CSEC 4200 Not Found | |
| CSEC 4300 | [0.0] | Course CSEC 4300 Not Found | |
| CSEC 4900 | [0.0] | Course CSEC 4900 Not Found | |
| CSEC 4901 | [0.0] | Course CSEC 4901 Not Found | |

B. Credits Not Included in the Major CGPA (8.5 credits)

| | | |
|---|---|---|
| **5. 1.0 credit in:** | | 1.0 |
| MATH 1007 [0.5] | Elementary Calculus I | |
| MATH 1104 [0.5] | Linear Algebra for Engineering or Science | |
| **6. 0.5 credit in:** | | 0.5 |
| STAT 2507 [0.5] | Introduction to Statistical Modeling I | |
| **7. 7.0 credits in** free electives | | 7.0 |
| Total Credits | | 20.0 |

New Resources

Faculty

Summary

New program Bachelor of Cybersecurity BCyber Honours.

Rationale

The School of Computer Science (SCS) is proposing a new Honours undergraduate degree: the Bachelor of Cybersecurity (BCyber). The program is designed to be a national magnet for high-achieving students who are strongly interested in a career in security. We believe this is feasible, and attractive to students, for the following reasons. 1. This will be the first program in Canada of its kind. 2. Security courses will be taught by members of one of the country's top research groups in the area, arguably the top amongst groups whose work spans the theory-practice spectrum. 3. There is a recent consensus that in computing-related areas of study, security has emerged as its own distinct area, alongside the other existing top-level areas of Computer Engineering (CE), Computer Science (CS), Information Systems, Information Technology (IT) and Software Engineering (SE). 4. Our experience with the Shopify internship partnership has shown both that it is possible to attract outstanding students to Carleton for a unique program. 5. Ottawa, in addition to having numerous software companies that have a core business interest in security, has, as the nation's capital, the main governmental organizations that have Cybersecurity as a primary focus. These include CSE (Communications Security Establishment), DND and the RCMP. The program's structure will provide for earlier, and more meaningful, co-op opportunities. 6. Since the degree includes most of the core of a standard CS (Computer Science) degree, it will not carry the risk for students of a new kind of degree program that is unknown to employers. 7. The program will have a strong cohort aspect, with limited enrolment and cohort-building components such as exclusive courses and course sections. 8. As has been successfully done with the Shopify internship program, the BCyber will be "front-loaded", using a compressed introduction that will make students employable in co-op positions after their first year.

Transition/Implementation

We do not expect the BCyber to draw significant numbers of students from the existing BCS security
stream, or the BCS in general. The specialization and uniqueness of this program will draw new students
who would otherwise go to a top Canadian CS university such as Waterloo, University of Toronto or UBC.
While it is likely some of the applicants to the BCS security stream would apply to the BCyber, such students would be competing in a nationally-drawn pool of high-achieving students who have a strong
commitment to focusing on security.
We also expect that a few students enrolling in the BCSec at the expense of the BCS will be more than
counterbalanced by the increased national visibility of the BCS that the BCyber will provide. This effect
has been demonstrated by two of our previous BCS initiatives: the game development stream and
Industrial Internship Option partnership with Shopify. Students often decided to come to Carleton for a
BCS because we offer attractive content, even if they were not particularly interested in the

# New Course Proposal

Date Submitted: 05/14/24 3:43 pm

## Viewing: CSEC 3999 : Co-operative Work Term

Last edit: 05/14/24 3:43 pm

Changes proposed by: nataliephelan

| | |
|---|---|
| Programs referencing this course | R-UG-COOP-B.C.Sec. Admission and Continuation Requirements |

### In Workflow

1. **COMP ChairDir UG**
2. **COMP FCC**
3. **COMP FBoard**
4. **PRE SCCASP**
5. SCCASP
6. SQAPC
7. Senate
8. PRE CalEditor
9. Banner

### Approval Path

1. 05/17/24 11:52 am Michel Barbeau (michelbarbeau): Approved for COMP ChairDir UG
2. 05/17/24 11:56 am Michel Barbeau (michelbarbeau): Approved for COMP FCC
3. 05/17/24 11:56 am Michel Barbeau (michelbarbeau): Approved for COMP FBoard

| | |
|---|---|
| Effective Date | 2025-26 |
| Workflow | majormod |
| New Resources | No New Resources |
| Level | Undergraduate |
| Course Code | CSEC |
| Course Number | 3999 |
| Title | Co-operative Work Term |
| Title (short) | Co-op Work Term |
| Faculty | Faculty of Science |
| Academic Unit | School of Computer Science |

| | |
|---|---|
| Credit Value | 0.0 |
| Special/Selected Topics | Not Applicable |
| Significant Experiential Learning | Co-op |
| Course Description | |
| Prerequisite(s) | |
| Class Format | |
| Precluded Courses | |
| Also listed as | |
| Piggybacked Courses | |
| Grade Mode | Satisfactory/Unsatisfactory |
| Schedule Type | *Work Term<br>*May constitute a major modification under Carleton's IQAP. Please consult https://carleton.ca/viceprovost/major-minor-modifications/ for more details. |
| Unpaid Placement | No |
| Summary | Assoc with NP TBD-2258 Cybersecurity BCSec |
| Rationale for new course | |
| Course reviewer comments | |

Key: 10953
Not an admin

# AbdelRahman Abdou

Assistant Professor, School of Computer Science, Carleton University, Canada.
Co-director, Carleton Internet Security Lab (CISL).
✉ | HP5130 – 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6.
🖮 | https://people.scs.carleton.ca/~abdou/ 🖃 | abdou@carleton.ca


## Academic Experience

Dec 2018–Present

Carleton University, Ottawa, Canada.
Assistant Professor—School of Computer Science.
Co-director, Carleton Internet Security Lab (CISL): https://cisl.carleton.ca/.

Dec 2017–Nov 2018

ETH Zürich, Zürich, Switzerland.
Postdoctoral Researcher—Institute of Information Security, Department of Computer Science.

*Supervisor:* Srdjan Čapkun.
*Research objectives:* Authentication and Internet Security, System Security, Distance Verification in UWB.

Sep 2015–Nov 2017

Carleton University, Ottawa, Canada.
Post-Doctoral Fellow—School of Computer Science.

*Supervisor:* Paul C. Van Oorschot.
*Research objectives:* Improving client authentication, reinforcing SSL/TLS, analyzing software-defined networks.

Jan 2011–Aug 2015

Carleton University, Ottawa, Canada.
Teaching and Research Assistant—Department of Systems and Computer Engineering.

Mar 2010–Dec 2010

Arab Academy for Science and Technology (AAST), Alexandria, Egypt.
Assistant Lecturer—Department of Computer Engineering.

Sep 2007–Feb 2010

Arab Academy for Science and Technology (AAST), Alexandria, Egypt.
Graduate Teaching Assistant—Department of Computer Engineering.

## Education

Jan 2011–Jun 2015

Carleton University, Ottawa, Canada.
PhD—Systems and Computer Engineering

*Thesis title:* Internet Location Verification: Challenges and Solutions.
*Supervisors:* Ashraf Matrawy and Paul C. Van Oorschot.
*External Examiner:* Urs Hengartner, University of Waterloo.
*Major:* Computer & Broadband Networks; *Minor:* Computer Architecture & Organization.

Sep 2007–Feb 2010

Arab Academy for Science and Technology (AAST), Alexandria, Egypt.
M.Sc.—Computer Engineering

*Thesis title:* Decision Engines for Multi-hop Ad-hoc Networks.
*Supervisors:* Mohamad Abou El-Nasr and Ossama Ismail.
*Language of Instruction:* English.

Sep 2002–Jul 2007

Arab Academy for Science and Technology (AAST), Alexandria, Egypt.
B.Sc.—Computer Engineering

*Honorary project title:* An Overlay P2P Network for Educational Digital Libraries.
*Excellent with Honour; Ranked $2^{nd}$ in class.*
*Language of Instruction:* English.

## Research Interests

I am interested in Internet Security. This includes topics spanning Web security, TLS, DNS security, authentication, secure BGP, secure Internet geolocation, Internet censorship, and SDN security. I am also interested in using Internet measurements to understand and solve problems related to Internet systems' security.

## Research Funding

2023 Human-Centric Cybersecurity Partnership (HC2P)—$50,000. co-PI, my share: $25,000
I am a member of Human-Centric Cybersecurity Partnership (HC2P)—a PAN-Canadian research network.

2022 ISED Cyber Security Innovation Network (CSIN).
I am a member of The National Cybersecurity Consortium (NCC), which is a PAN-Canadian network that was awarded $80 million funding for security research.

2019 NSERC Discovery Launch Supplement—$12,500.
School of Computer Science, Carleton University, Ottawa, ON, Canada.

2019 NSERC Discovery Grant—$168,000 ($28,000/year for 6 years).
School of Computer Science, Carleton University, Ottawa, ON, Canada.

## Recognitions

2017 Distinguished Paper Award.
ACM Asia Conference on Computer and Communications Security (AsiaCCS), Abu Dhabi, UAE.

2014 Best Paper Award nomination.
IEEE Communications and Network Security (CNS), San Francisco, CA, USA.

2014 Student Travel Grant—$400.
IEEE CNS, San Francisco, CA, USA.

2012 Student Travel Grant—$445.
USENIX Security Symposium, Bellevue, WA, USA.

2011-2014 Graduate Scholarship—$26,200.
Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada.

2009 One of seven international teams selected for the MANIAC challenge.
Mobile Ad-hoc Networks Interoperability & Cooperation (MANIAC) challenge, TX, USA.

2007-2010 Graduate Engineering Studies Scholarship—M.Sc. Tuition Waiver.
Arab Academy for Science and Technology (AAST), Alexandria, Egypt.

2007 ICPC $7^{th}$ place award of 45 Arab and North African regional teams—IBM sponsored
ACM International Collegiate Programming Contest (ICPC), Alexandria, Egypt.

## Services to the Profession

### Technical Program Committee

2023 PC member
IEEE Symposium on Security and Privacy (S&P—*Oakland* 2024).

2022 PC member
IEEE Symposium on Security and Privacy (S&P—*Oakland* 2023).

2021 PC member
IEEE European Symposium on Security and Privacy (EuroS&P 2022).

2021 PC member
Workshop on Cyber Security Experimentation and Test (CSET 2021).

2020 PC member
IEEE European Symposium on Security and Privacy (EuroS&P 2021).

2020 PC member
USENIX Security Workshop on Cyber Security Experimentation and Test (CSET 2020).

2020 PC member
ACM Conference on Computer and Communications Security (CCS 2020).

2019 PC member
IEEE European Symposium on Security and Privacy (EuroS&P 2020).

2018 PC MEMBER
IEEE European Symposium on Security and Privacy (EuroS&P 2019).

2018 POSTER PC MEMBER
ACM Conference on Computer and Communications Security (CCS 2018).

## Journal Editorial Board

2020-present REVIEW EDITOR
Frontiers in Communications and Networks—Security, Privacy and Authentication.

## Journal Paper Reviewing

2023 REVIEWER
Transactions on Network Science and Engineering (TNSE)—IEEE.

2022 REVIEWER
Transactions on Network and Service Management (TNSM)—IEEE.

2022 REVIEWER
Security and Privacy magazine—IEEE.

2021 REVIEWER
Computing—Springer.

2020 REVIEWER
International Journal for the Computer and Telecommunications Industry—Elsevier Computer Communications.

2019 REVIEWER
Security and Privacy magazine (Special issue on EuroS&P 2019)—IEEE.

2019 REVIEWER
International Journal of Distributed Sensor Networks (IJDSN)—SAGE Journals.

2019 REVIEWER
Security and Privacy magazine (Special issue on IoT Security and Privacy)—IEEE.

2018 REVIEWER
International Journal for the Computer and Telecommunications Industry—Elsevier Computer Communications.

2018 REVIEWER
Wireless Communications and Networking—Springer EURASIP.

2018 REVIEWER
International Journal of Distributed Sensor Networks (IJDSN)—SAGE Journals.

2018 REVIEWER
Transactions on Network and Service Management (TNSM)—IEEE.

2017 REVIEWER
International Journal for the Computer and Telecommunications Industry—Elsevier Computer Communications.

2017 REVIEWER
Transactions on Dependable and Secure Computing (TDSC)—IEEE.

## Conference Paper Reviewing

2019 REVIEWER
ACM Conference on Mobile Computing and Networking (MobiCom).

2019 REVIEWER
Network and Distributed System Security Symposium (NDSS).

2018 REVIEWER
ACM Conference on Computer and Communications Security (CCS).

2018 REVIEWER
Symposium on Research in Attacks, Intrusions and Defenses (RAID).

2018 REVIEWER
ACM Conference on Mobile Computing and Networking (MobiCom).

2018 Reviewer
USENIX Security Symposium.

2018 Reviewer
IEEE Conference on Communications and Network Security (CNS).

2017 External reviewer
ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT).

2017 Reviewer
IEEE Conference on Communications and Network Security (CNS).

2016 Reviewer
IEEE Conference on Communications and Network Security (CNS).

2016 Reviewer
IEEE International Conference on Communications (ICC).

2014 External reviewer
Annual Computer Security Applications Conference (ACSAC).

## Graduate Student Committees

### As Committee Examiner

2023 MCS Project Committee (Examiner), Carleton University, Canada
Ming Lei, School of Computer Science (Aug 4th)

2023 PhD Comprehensive Exam Committee (Supervisor), Carleton University, Canada
Hussaini Zubairu, Carleton School of Information Technology (Aug 3rd)

2023 PhD Proposal Examination Committee (Supervisor), Carleton University, Canada
Ali Jahromi, School of Computer Science (Jul 20th)

2022 MCS Project Committee (Examiner), Carleton University, Canada
Heli Alpeshkumar Patel, School of Computer Science (Dec 14th)

2022 PhD Comprehensive Exam Committee (Examiner–Major Subject in Security), Carleton University, Canada
Ali Jahromi, School of Computer Science (Nov 16th)

2022 PhD Thesis Committee (Internal Examiner), Carleton University, Canada
Christopher Bellman, School of Computer Science (Aug 16th)

2022 PhD Comprehensive Exam Committee (University Examiner), Carleton University, Canada
Emmanuel Alalade, Carleton School of Information Technology (Apr 28th and May 26th)

2022 MCS Thesis Committee (Internal Examiner), Carleton University, Canada
Muhammad Shafayat Oshman, School of Computer Science (Jan 5th)

2021 PhD Proposal Examination Committee (Internal Examiner), Carleton University, Canada
Hemant Gupta, School of Computer Science (Jun 1st)

2021 PhD Comprehensive Exam Committee (Examiner–Major Subject in Networks), University of Ottawa, Canada
Ahmed Omara, School of Electrical Engineering and Computer Science (Apr 28th)

2020 PhD Thesis Committee (Internal Examiner), Carleton University, Canada
Danish Sattar, Systems and Computer Engineering (Sep 11th)

2020 PhD Comprehensive Exam Committee (Examiner–Minor Subject in Networks), Carleton University, Canada
Hemant Gupta, School of Computer Science (Sep 4th)

2020 PhD Proposal Examination Committee (Internal Examiner), Carleton University, Canada
Christopher Bellman, School of Computer Science (May 7th)

2019 MCS Thesis Committee (Internal Examiner), Carleton University, Canada
Hemant Gupta, School of Computer Science (Jul 16th)

2019 PhD Proposal Examination Committee (Internal Examiner), Carleton University, Canada

Danish Sattar, Systems and Computer Engineering (May 23rd)

## As Committee Chair

2023 MCS Thesis Committee (Chair), Carleton University, Canada
Galen O'Shea, School of Computer Science (Apr 19th)

2022 MCS Thesis Committee (Chair), Carleton University, Canada
Gowthaman Sivakumaran, School of Computer Science (May 4th)

2019 MCS Thesis Committee (Chair), Carleton University, Canada
Reza Samanfar, School of Computer Science (Dec 19th)

2019 Master of Arts Examination Committee (Chair), Carleton University, Canada
Jessica Rocheleau, Human-Computer Interaction Unit (Aug 6th)

2019 M.A.Sc. Examination Committee (Chair), Carleton University, Canada
Nour Dabour, Human-Computer Interaction Unit (May 2nd)

2019 PhD Comprehensive Exam Committee (Chair), Carleton University, Canada
Lars Doyle, School of Computer Science (Jan 21st)

## University Services

2021-present Graduate Student Admissions Committee Member
A committee responsible for filtering out and processing tens of graduate student applications in the School of Computer Science.

2020-2022 Tenure and Promotion Committee Member, Carleton University, Canada
A committee responsible for processing tenure and promotion applications in the School of Computer Science. We also reviewed and updated tenure and promotion regulations for the Collective Agreement, including soliciting input from external reviewers regarding the new regulations.

2019, 2023 Co-op report-grading committee, Carleton University, Canada
A committee responsible for grading co-op reports, and corresponding feedback to students.

2019 Faculty Hiring Committee, Carleton University, Canada
Member of the faculty hiring committee for two tenure-track security positions at the School of Computer Science. Both positions were successfully filled, plus one additional hire.

2010 ABET Committee Member, AAST, Alexandria, Egypt.
A committee responsible for ensuring the Computer Engineering department's conformity to the conditions of the Accreditation Board for Engineering and Technology (ABET).

2010 Examination Committee Member, AAST, Alexandria, Egypt.
A committee responsible for organizing the department's final exams and examination rooms, scheduling invigilators, and handled distribution and collection of examination booklets.

2010 Head of the Timetabling committee, AAST, Alexandria, Egypt.
A committee responsible for the Computer Engineering department's timetabling. This includes timetables for: courses, classrooms, instructors, and teaching assistants.

2007–2009 Timetabling Committee Member, AAST, Alexandria, Egypt.
See description of the Committee's responsibilities above.

2008–2010 Academic Advising, Arab Academy for Science and Technology (AAST)
I was selected by the Department Chair to be the Academic Advisor for a group of 20 undergraduate students in need for special advising. Towards building their educational plans, those students had growing unresolved course and registration conflicts accumulating over the years.

2009 EOI programming competition, problem setting committee, Alexandria, Egypt.
I was among a committee of 5 members responsible for writing the problem set of the Egyptian Olympiads in Informatics (EOI), a national programming competition organized annually for the top 100 programmers attending middle and high schools or freshmen (ranging 11-20 years old).

## Teaching Experience

Assistant Professor, School of Computer Science, Carleton University
*Courses:*
- Operating Systems (COMP 3000) — F'23
- Internet Measurements and Security (COMP 5500) — F'23
- Principles of Computer Networks (COMP 3203) — W'21, W'22, W'23, W'24
- Computer Systems Security (COMP 4108) — F'19, W'20, W'21, F'21, F'22
- Internet Measurements and Security (COMP 5900) — W'19, W'20, F'20, F'21, F'22

Teaching Assistant, Institute of Information Security, ETH Zürich
*Courses:*
- Information Security — Spring 2018
- Current Topics in Information Security — Fall 2018

Teaching Assistant, Systems and Computer Engineering, Carleton University
*Courses:*
- Communication Theory — Summer 2015
- Introduction to Programming and Problem Solving (C++) — Fall 2014
- Computer Organization (Assembly) — Summer 2011, 2012, 2014
- 3D Computer Animation — Fall 2013
- Foundation of Imperative Programming — Summer 2013

Assistant Lecturer, College of Engineering, AAST
*Courses:*
- Computer Networks — Summer 2010, Fall 2010
- Object Oriented Programming — Fall 2010

Assistant Lecturer, College of Computing and Information Technology, AAST
*Courses (Part of an Information Systems Diploma):*
- Data Structures — Fall 2010
- Discrete Mathematics — Fall 2010

Graduate Teaching Assistant, College of Engineering, AAST
*Courses:*
- Introduction to Computers — Fall 2007
- Digital Logic Design — Winter 2008, 2010
- Digital Systems Design and VHDL — Winter 2008
- Data and Computer Communication — Fall 2007, Winter 2008
- Computer Networks — Fall 2008, Winter 2009, 2010, Summer 2009
- Programming Applications — Fall 2009
- Object Oriented Programming — Fall 2008, 2009, Winter 2009, 2010
- Computing Algorithms — Fall 2008, 2009, Winter 2009

Lecturer, Egyptian Olympiads in Informatics (EOI)
I was the course instructor for *Algorithms for the EOI*, teaching a class of 20 students (ages between 11 and 20) competing in the national EOI programming contests. Besides introducing them to the C programming language, the course covers a wide range of topics including: Searching and Sorting, Dynamic Programming, Data Structures, Divide and Conquer, Graph Theory, and Computational Geometry.

Private Tutor
As a senior undergraduate student, I provided individual and group private tutoring to second and third year undergraduate students.
*Courses:*
- Object Oriented Programming — Fall 2006
- Structured Programming — Winter 2006

## Industrial Collaboration

2016-2018 NBCUniversal (Los Angeles, CA, USA)
Devising and testing Internet location verification technologies on Akamai network for geographically-oriented NBC content distribution.

2013 PlaceSpeak Inc, Vancouver, BC, Canada
As part of the NSERC Engage program, I worked on a 6-months project in collaboration with PlaceSpeak to analyze privacy and security weaknesses of the W3C geolocation API. I was responsible for writing parts of the Engage Grant, including a technical summary of potential vulnerabilities and privacy leakages.

## Mentoring and Supervision

### Graduate Students

2023-present Ghazaleh Shirvani—PhD student.
School of Computer Science, Carleton University
Thesis title: TBD.

2023-present Patrick Guo—MCS student.
School of Computer Science, Carleton University
Thesis title: TBD.

2022-present Hussaini Zubairu—PhD student (co-supervisor: Ashraf Matrawy).
School of Information Technology, Carleton University
Thesis title: TBD.

2022-present Abdelrahman Soliman—MCS student
School of Computer Science, Carleton University
Thesis title: TBD.

2022-present Ethan Thompson—MCS student
School of Computer Science, Carleton University
Thesis title: TBD.

2022-present Nareen Khurshid—MCS student
School of Computer Science, Carleton University
Thesis title: TBD.

2021-present Ali Sadeghi Jahromi—PhD student (co-supervisor: Paul Van Oorschot).
School of Computer Science, Carleton University
Thesis title: TBD.

2019-2021 Ali Sadeghi Jahromi—MCS student
School of Computer Science, Carleton University
Thesis title: Survey and Evaluation of Secure-DNS Alternatives.

2020-2021 Christopher Bennett—MCS student (co-supervisor: Paul Van Oorschot).
School of Computer Science, Carleton University
Thesis title: Search Engines that Scan for Internet-connected Services: Classification and Empirical Study.

2018-2019 Nicole Thurnherr—M.Sc. student
Institute of Information Security, ETH Zürich
Thesis title: Evaluating Authentication Completeness.

2018-2019 Michele Roberti—M.Sc. student
Institute of Information Security, ETH Zürich
Thesis title: Scalable Location Verification for Internet Clients.

2018-2019 Mridula Singh—PhD student (co-supervisor: Srdjan Čapkun).
Institute of Information Security, ETH Zürich
Thesis title: Cross-Layer Design of Securing Positioning.
Current Position: Faculty Member at CISPA Helmholtz Center for Information Security.

### Undergraduate Students

2023 Patrick Guo—Honours Project.
School of Computer Science, Carleton University
Project title: Analyzing Domain Group Registration as Mitigation for Phishing Attacks.

2022 Matthew Nitschke—Honours Project.
School of Computer Science, Carleton University
Project title: Investigating the Vulnerabilities of DNS over HTTPS.

2022 Salah Al-Zabet—Honours Project.
School of Computer Science, Carleton University
Project title: Environments of online hate and harassment - content based filtering.

2022 Ethan Thompson—Honours Project.
School of Computer Science, Carleton University
Project title: Certificate Cross-Signing Analysis.

2021-2022 Devan Andersen—Honours Thesis.

School of Computer Science, Carleton University
Thesis title: A New Approach to Censorship-Circumvention: Computing and Compiling Decentralized Censored Websites.

2021 Nareen Khurshid—Honours Project.
School of Computer Science, Carleton University
Project title: Analyzing Game Security Software and System Behaviour.

2021 Tan Tran—Honours Project.
School of Computer Science, Carleton University
Project title: Threshold Cryptosystem Scheme: Secure Delegation Through the Distribution of the Private Key Across Multiple CDN Servers.

2020 Mohamad Cheaito—Honours Project.
School of Computer Science, Carleton University
Project title: Browser Based Crypto-jacking Systems.

2020 Jegan Purushothaman—Honours Project.
School of Computer Science, Carleton University
Project title: Study on Root Certificate Stores.

2020 Matthew Talbot—Honours Project.
School of Computer Science, Carleton University
Project title: Creating a Stealthy Backdoor.

2020 Quinn Mcgarry—Honours Project.
School of Computer Science, Carleton University
Project title: Understanding Vulnerability Remediation Obstacles of System Administrators.

2020 Farhoud Talebi—Honours Project.
School of Computer Science, Carleton University
Project title: Pervasive Surveillance Tools.

2020 Sanjida Sanwar—Honours Project.
School of Computer Science, Carleton University
Project title: Web authentication.

2019 Tyler Despatie—Honours Project.
School of Computer Science, Carleton University
Project title: Web certificates.

2019 George Li—Dean's Summer Research Intern (DSRI) (co-supervisor: Paul Van Oorschot).
School of Computer Science, Carleton University
Project title: Analyzing Certificate Transparency.

2015 Kyle Thompson—$3^{rd}$ year undergraduate (co-supervisor: Paul Van Oorschot).
School of Computer Science, Carleton University
Project title: Frameworks for Systematic Evaluations of Web-authentication Schemes

2007–2008 Coaching the AAST programming contestants, Regional Informatics Centre (RIC)
I was responsible for coaching the AAST's team to compete in the regional (Arab and North African Region) programming contest of the ACM's annual International Collegiate Programming Contest (ICPC). Coaching was both technical and through frequent motivational speeches and activities as they faced the challenges of learning complex Algorithms and problem solving techniques.

## Presentations, Talks and Guest Lectures

2023 Why do Internet Devices Remain Vulnerable? A Survey with System Administrators
NDSS Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2023), San Diego, USA.

2021 Use-cases and Challenges for Secure Delegation Over the Internet
Invited talk (Madiba Security Research Group, Concordia University, Montreal, Canada; host: Mohammad Mannan), Online.

2021 Latest on Web-Authentication
Invited talk (Tech Session with Universal Film Technology, NBC Universal Pictures, Los Angeles, USA; host: Alex Olugbile), Online.

2020 Cyber Security Panel
Invited panel (Project Technical Conference), Online.

2019 Computer Science and Internet Security

Invited panel (Project Technical Conference), University of Ottawa, Ottawa, ON, Canada.

2019 Challenges and Methods for Secure Ranging and Positioning of Internet-Connected Systems
Invited talk (Département d'Informatique et d'Ingénierie, host: Mohand Allili), Université du Québec en Outaouais, Gatineau, QC, Canada.

2018 Secure Internet Measurements for Verified Location Information
Invited talk (School of Computer Science, host: Doug Howe), Carleton University, Ottawa, ON, Canada.

2018 Secure Internet Measurements for Verified Location Information
Invited talk (Electrical Engineering and Computer Science, host: Jarek Gryz), York University, Toronto, ON, Canada.

2018 From Blockchains to Anonymity Networks
Invited talk (Privacy and Security group, host: Carlisle Adams), University of Ottawa, Ottawa, ON, Canada.

2017 Server Location Verification (SLV): Augmenting TLS using Servers' Physical Location
USENIX Security Lightning Talk (USENIX Security 2017), Vancouver, BC, Canada.

2017 Towards Securely Verifying Location Claims on the Internet
Invited talk (IBM Research, host: David Barrera), IBM Zürich, Zürich, Switzerland.

2017 Towards Securely Verifying Location Claims on the Internet
Invited talk (Inst. of Info. Security, host: Srdjan Čapkun), ETH Zürich, Zürich, Switzerland.

2017 Challenges and Solutions to Secure Internet Geolocation
Invited talk online (School of Computing Science, host: Mohamed Hefeeda), Simon Fraser University, Burnaby, BC, Canada.

2017 Challenges and Solutions to Secure Internet Geolocation
Invited talk (Computer System Lab, host: David Lie), University of Toronto, Toronto, ON, Canada.

2017 Accurate Manipulation of Delay-based Internet Geolocation
ACM Asia Conference on Computer and Communications Security (AsiaCCS). Abu Dhabi, UAE.

2016 The Role of Internet Measurements in Security
Online talk (1hr), Security Compass, Canada.

2015 Designing Secure Networking and Computer Systems
Guest lecture (1.5hr) for SYSC5500 graduate course, Carleton University, Canada.

2014 Location Verification on the Internet
IEEE Conference on Communications and Network Security (CNS). San Francisco, CA, USA.

2013 Foundations of Imperative Programming
Guest lecture (3hr) for SYSC2006 undergraduate course, Carleton University, Canada.

2013 Toward Location-Verification of Web-Clients
Internetworked Systems Security Network (ISSNet) workshop. Victoria, BC, Canada.

2013 Reflecting on Ralph Merkle's original public-key protocol
Two-minute madness talk, NSERC ISSNet summer security week. Calgary, AB, Canada.

2013 A Study of the W3C Geolocation API
Presented to the CTO and employees of PlaceSpeak Inc. Vancouver, BC, Canada.

2010 Analysis and Design of Computer Networks
Guest lecture (3hr) for CC733 graduate course, AAST, Egypt.

2010 Computer Engineering: Career Paths
The college of Engineering at the AAST, Egypt organizes a series of introductory sessions for each department, to assist freshmen in identifying their major/minor specialities. I was selected to give this presentation, introducing Computer Engineering as a career path.

2009 A Novel Forwarding/Dropping Decision Engine for Wireless Multi-hop Ad-hoc Networks
International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2009). Crystal City, VA, USA.

2009 The Mongoose Strategy
The MANIAC challenge, in conjunction with IEEE PerCom. Galveston, TX, USA.

## Journal Publications (Refereed)

8. F. Alaca, A. Abdou, P.C. van Oorschot. "Comparative Analysis and Framework Evaluating Mimicry-Resistant and Invisible Web Authentication Schemes". IEEE Transactions on Dependable and Secure Computing (TDSC, Vol.18. Num.2. pp:534-549. 2021). https://ieeexplore.ieee.org/document/8685680

7. A. Abdou, P.C. van Oorschot, T. Wan. "A Framework and Comparative Analysis of Control Plane Security of SDN and Conventional Networks". IEEE Communications Surveys and Tutorials (COMST, Vol.20. Num.4. pp:3542-3559. 2018). https://ieeexplore.ieee.org/abstract/document/8362609

6. A. Abdou, P.C. van Oorschot. "Server Location Verification (SLV) and Server Location Pinning: Augmenting TLS Authentication". ACM Transactions on Privacy and Security (TOPS, Vol.21. Num.1. pp:1:1-1:26. 2017). https://dl.acm.org/citation.cfm?id=3139294

5. A. Dabir, A. Abdou, A. Matrawy. "A Survey on Forensic Event Reconstruction Systems". International Journal of Information and Computer Security (IJICS, Vol.9. Num.4. pp:337-360. 2017). http://www.inderscience.com/info/inarticle.php?artid=87565

4. A. Abdou, A. Matrawy, P.C. van Oorschot. "CPV: Delay-based Location Verification for the Internet". IEEE Transactions on Dependable and Secure Computing (TDSC, Vol.14. Num.2. pp:130-144. 2017). http://ieeexplore.ieee.org/document/7145434/
*See* Press and Miscellaneous Coverage *section below.*

3. A. Abdou, A. Matrawy, P.C. van Oorschot. "Location Verification of Wireless Internet Clients: Evaluation and Improvements". IEEE Transactions on Emerging Topics in Computing (TETC, Vol.5. Num.4. pp:563-575. 2017). http://ieeexplore.ieee.org/document/7565495/

2. A. Abdou, A. Matrawy, P.C. van Oorschot. "Accurate One-Way Delay Estimation with Reduced Client-Trustworthiness". IEEE Communications Letters (CL, Vol.19. Num.5. pp:735-738. 2015). http://ieeexplore.ieee.org/document/7056556/

1. A. Abdou, A. Matrawy, P.C. van Oorschot. "Taxing the Queue: Hindering Middleboxes from Unauthorized Large-Scale Traffic Relaying". IEEE Communications Letters (CL, Vol.19. Num.1. pp:42-25. 2015). http://ieeexplore.ieee.org/document/6881620/

## Conferences and Workshop Publications (Refereed)

13. J. Breton, A. Abdou. "Applying Accessibility Metrics to Measure the Threat Landscape for Users with Disabilities". NDSS Workshop on Measurements, Attacks, and Defenses for the Web (NDSS MADWeb 2023). https://madweb.work/papers/2023/madweb23-breton.pdf

12. T. Bondar, H. Assal, A. Abdou. "Why do Internet Devices Remain Vulnerable? A Survey with System Administrators". NDSS Workshop on Measurements, Attacks, and Defenses for the Web (NDSS MADWeb 2023). https://madweb.work/papers/2023/madweb23-bondar.pdf

11. J. Purushothaman, E. Thompson, A. Abdou. "Certificate Root Stores—An Area of Unity or Disparity?". Workshop on Cyber Security Experimentation and Test (CSET 2022). https://cset22.isi.edu/slides/rootstore.pdf

10. W. Findlay, A. Abdou. "Characterizing the Adoption of Security.txt Files and their Applications to Vulnerability Notification". NDSS Workshop on Measurements, Attacks, and Defenses for the Web (NDSS MADWeb 2022). https://www.ndss-symposium.org/wp-content/uploads/madweb2022_23014_paper.pdf

9. E. Ulqinaku, H. Assal, A. Abdou, S. Chiasson, S. Čapkun. "Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols". USENIX Security Symposium (2021). https://www.usenix.org/system/files/sec21-ulqinaku.pdf

8. A. Jahromi, A. Abdou. "Comparative Analysis of DoT and HTTPS Certificate Ecosystems". NDSS Workshop on Measurements, Attacks, and Defenses for the Web (NDSS MADWeb 2021). https://madweb.work/preprints/madweb21-paper27-pre_print_version.pdf

7. C. Bennett, A. Abdou, P.C. van Oorschot. "Empirical Scanning Analysis of Censys and Shodan". NDSS Workshop on Measurements, Attacks, and Defenses for the Web (NDSS MADWeb 2021). https://madweb.work/preprints/madweb21-paper9-pre_print_version.pdf

6. L. Chuat, A. Abdou, R. Sasse, C. Sprenger, D. Basin, A. Perrig. "SoK: Delegation and Revocation, the Missing Links in the Web's Chain of Trust". IEEE European Symposium on Security & Privacy (EuroS&P 2020). https://netsec.ethz.ch/publications/papers/sok-delegation-revocation.pdf

5. M. Singh, P. Leu, A. Abdou, S. Čapkun. "UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband". USENIX Security Symposium (2019). https://www.usenix.org/system/files/sec19-singh.pdf

4. A. Abdou, A. Matrawy, P.C. van Oorschot. "Accurate Manipulation of Delay-based Internet Geolocation". ACM Asia Conference on Computer and Communications Security (AsiaCCS 2017). https://dl.acm.org/citation.cfm?id=3052993
*Distinguished Paper Award.*

3. A. Abdou, D. Barrera, P.C. van Oorschot. "What lies beneath? Analyzing automated SSH brute-force attacks". Springer LNCS (Passwords 2015). http://link.springer.com/chapter/10.1007%2F978-3-319-29938-9_6

2. A. Abdou, A. Matrawy, P.C. van Oorschot. "Location Verification on the Internet: Towards Enforcing Location-aware Access Policies Over Internet Clients". IEEE Conference on Communications and Network Security (CNS 2014). http://ieeexplore.ieee.org/document/6997484/
*Top 4% of submissions; Nominated for Best Paper award; See* Press and Miscellaneous Coverage *section below.*

1. A. Abdou, M. Abou El-Nasr, O. Ismail. "A Novel Forwarding/Dropping Decision Engine for Wireless Multi-hop Ad-hoc Networks". International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2009). http://ieeexplore.ieee.org/document/5365432/
*See* Press and Miscellaneous Coverage *section below.*

## Extended Poster Abstracts (Refereed)

1. A. Abdou, A. Matrawy, P.C. van Oorschot. "Verifying Geographic Location Presence of Internet Clients". Two page refereed Abstract and a Poster in the $37^{th}$ IEEE Symposium on Security and Privacy (S&P). San Jose, CA, USA. May 2016

## Technical Reports, Posters, and Magazine Commentaries

- S.G. Morkonda, A. Abdou. "Work in progress: Identifying Two-Factor Authentication Support in Banking Sites". Cornell University, arXiv:2202.06459, February 2022.
- J. Purushothaman, A. Abdou. "Certificate Root Stores: An Area of Unity or Disparity?". Cornell University, arXiv:2110.11488, October 2021.
- E. Ulqinaku, H. Assal, A. Abdou, S. Chiasson, S. Čapkun. "Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols". ePrint archives, Oct 2020.
- L. Chuat, A. Abdou, R. Sasse, C. Sprenger, D. Basin, A. Perrig. "Proxy Certificates: The Missing Link in the Web's Chain of Trust". Cornell University, arXiv:1906.10775, June 2019.
- A. Abdou, P.C. van Oorschot. "Secure Client and Server Geolocation Over the Internet". USENIX ;login: magazine, March 2018 issue.
- F. Alaca, A. Abdou, P.C. van Oorschot. "Comparative Analysis and Framework Evaluating Mimicry-Resistant and Invisible Web Authentication Schemes". Cornell University, arXiv:1708.01706, August 2017.
- A. Abdou, P.C. van Oorschot, T. Wan. "A Framework and Comparative Analysis of Control Plane Security of SDN and Conventional Networks". Cornell University, arXiv:1703.06992, March 2017.
- A. Abdou, P.C. van Oorschot. "Server Location Verification and Server Location Pinning: Augmenting TLS Authentication". Cornell University, arXiv:1608.03939, August 2016.
- A. Abdou, A. Matrawy, P.C. van Oorschot. "On the Evasion of Delay-Based IP Geolocation". Carleton University Technical Report, June 2014.
- Carleton University Research Team. "A Study of the W3C Geolocation API". NSERC Engage project Technical Report, July 2013.
- A. Abdou, S. Neti. "Rump session of the $21^{st}$ USENIX Security Symposium". A summary in USENIX ;login: magazine, December 2012 issue.
- A. Abdou, A. Matrawy, P.C. van Oorschot. "Internet Geolocation: An Adversarial Perspective". A poster in the $4^{th}$ annual ISSNet Workshop. Kingston, ON, Canada. 2012.

## Press and Miscellaneous Coverage

2018

- APNIC Internet Registry blog
  Securing Internet geolocation: the basics
  Securing Internet geolocation: Client Presence Verification
  Securing Internet geolocation: Server Location Verification

2016

- The Globe and Mail
  Canadian researcher proposes new way to shut down Netflix 'content tourists'
- TechRepublic
  Researchers devise method to detect location spoofing by calculating network delays
- reddit
  Canadian researcher proposes new way to shut down Netflix 'content tourists'
- Slashdot
  How To Defeat VPN Location-Spoofing By Mapping Network Delays
- Schneier on Security
  Interesting research: Determining Physical Location on the Internet
- VPN Service Point
  Why The VPN Era Can Come To An End
- TechVibes
  Canadian Researcher Thinks He Can Help Netflix Stop People Accessing Other Countries' Libraries
- TheStack
  How to defeat VPN location-spoofing by mapping network delays
- Carleton Now
  Carleton researchers tackle computer location fraud

2014

- Quarterly cybersecurity knowledge digest of SERENE-RISC Smart Security Network
  Can I check if you are where you say you are online?

2009

- The Bradley Department of Electrical and Computer Engineering, VirginiaTech
  Global MANIACs compete in futuristic wireless network [p.35]

NSERC CRSNG

Canadian Common CV commun canadien

Protected when completed

This is a draft version only. Do not submit to any funding organization. Only the final version from the History page can be submitted.

---


## Professor Michel Barbeau

Correspondence language: English


## Contact Information

The primary information is denoted by (*)


### Address

Primary Affiliation (*)

School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa Quebec K1S 5B6
Canada

### Telephone

| | |
|---|---|
| Work (*) | 613-520-4333 |

### Email

| | |
|---|---|
| Work (*) | barbeau@scs.carleton.ca |

# Professor Michel Barbeau

## Language Skills

| Language | Read | Write | Speak | Understand | Peer Review |
|---|---|---|---|---|---|
| English | Yes | Yes | Yes | Yes | Yes |
| French | Yes | Yes | Yes | Yes | Yes |

## Degrees

- 1991/7 Doctorate, Computer Science, Université de Montréal
- 1987/6 Master's Thesis, Computer Science, Université de Montréal
- 1985/5 Bachelor's, Computer Science, Université de Sherbrooke

## Recognitions

2021/12
Best paper
European Alliance for Innovation (EAI)
Prize / Award
Recognizes the best paper of the conference.

2019/9
Xanadu Software Competition - Research award - 2nd place
Xanadu, Toronto, CANADA
Prize / Award
Demonstrating creative and exciting uses of open-source software that makes quantum computers more accessible

## User Profile

Research Specialization Keywords: Ad Hoc Network, Cognitive Radio Network, Communication Network, Network Security, Quantum Communications, Quantum Network, Software Defined Radio, Underwater Acoustic Network, Wireless Computer Network, Wireless Security

## Employment

2002/7
Professor
School of Computer Science, Carleton University
Full-time, Professor
Tenure Status: Tenure

| | |
|---|---|
| 2020/7 - 2025/6 | Director<br>School of Computer Science, Carleton University<br>Full-time, Term, Professor<br>Tenure Status: Non Tenure Track<br>Department's chair |
| 2019/7 - 2020/6 | Interim Director<br>School of Computer Science, Carleton University<br>Full-time, Term, Professor<br>Tenure Status: Non Tenure Track<br>Department's Chair |
| 2017/7 - 2018/6 | Assistant Dean (Recruitment & Retention)<br>Faculty of Science, Carleton University<br>Full-time, Term<br>Tenure Status: Non Tenure Track |
| 2017/7 - 2017/6 | Associate Director (Recruitment & Outreach)<br>School of Computer Science, Carleton University<br>Full-time, Term<br>Tenure Status: Non Tenure Track |
| 2013/7 - 2014/6 | Interim Director<br>School of Computer Science, Carleton University<br>Full-time, Term, Professor<br>Tenure Status: Non Tenure Track<br>Department's Chair |
| 2003/7 - 2009/6 | Associate Director<br>School of Computer Science, Carleton University<br>Full-time, Term, Professor<br>Tenure Status: Non Tenure Track<br>Undergraduate advisor, creation of a new program in computer games, recruitment of new undergraduate students |
| 2000/1 - 2002/6 | Associate Professor<br>School of Computer Science, Carleton University<br>Full-time, Associate Professor<br>Tenure Status: Tenure |
| 1994/6 - 1999/12 | Associate Professor<br>Mathematiques et informatique, Université de Sherbrooke<br>Full-time, Associate Professor<br>Tenure Status: Tenure |
| 1991/6 - 1994/5 | Assistant Professor<br>Mathematiques et informatique, Université de Sherbrooke<br>Full-time, Assistant Professor<br>Tenure Status: Tenure Track |

## Student/Postdoctoral Supervision

**Bachelor's Honours [n=12]**

2022/5 - 2022/8
Principal Supervisor
Tiffany Lau (Completed) , Carleton University
Thesis/Project Title: Explainable Artificial Intelligence and Quantum Machine Learning
Present Position: Student, Carleton University

2021/9 - 2022/4
Principal Supervisor
Yannick Beaupré (Completed) , Carleton University
Thesis/Project Title: Underwater Confidential Communications
Present Position: IT Security Analyst, Canadian Deposit Insurance Corporation (CIDC)

2021/9 - 2022/5
Principal Supervisor
Iain Burge (Completed) , Carleton University
Thesis/Project Title: Quantum Reinforcement Learning and Grover's Algorithm with Applications to Cyber-Physical Security
Present Position: Student, Carleton University

2021/5 - 2021/12
Principal Supervisor
Ammar Tosun (Completed) , Carleton University
Thesis/Project Title: 2D and 3D Visualization of Drone Collected 5G Received Signal Strength Data
Present Position: Backend engineer, NASDAQ

2021/1 - 2021/4
Principal Supervisor
Anonyous (Completed) , Carleton University
Thesis/Project Title: Analysis of Variational Circuits in Quantum Machine Learning
Present Position: Software Developer

2021/1 - 2021/4
Principal Supervisor
Haonan Zhang (Completed) , Carleton University
Thesis/Project Title: 5G GNU Radio
Present Position: Software Developer

2018/9 - 2018/12
Principal Supervisor
Alexkumar Patel (Completed) , Carleton University
Thesis/Project Title: GNU Radio: Decoding FT8 Protocol - Forward Error Correction
Present Position: Software Developer

2018/1 - 2018/4
Principal Supervisor
Rui Li (Completed) , Carleton University
Thesis/Project Title: Facial Age and Gender Recognition
Present Position: Software Developer

2017/9 - 2017/12
Principal Supervisor
Jean elie Jean-gilles (Completed) , Carleton University
Thesis/Project Title: shmPi: Smart Home Monitoring Using the Internet of Things
Present Position: Software Developer

2017/9 - 2017/12
Principal Supervisor
Coco Chen (Completed) , Carleton University
Thesis/Project Title: Smart Traveling Application
Present Position: Software Developer

2017/5 - 2017/8
Principal Supervisor
Hassan Amri (Completed) , Carleton University
Thesis/Project Title: Wireless Management Tool for AREDN
Present Position: Software Developer

2017/1 - 2017/4
Principal Supervisor
Kyle Thompson (Completed) , Carleton University
Thesis/Project Title: Anonymous Instant Messaging via P2P Onion Routing
Present Position: Software Developer

**Master's Thesis [n=4]**

| | |
|---|---|
| 2022/5 - 2023/5<br>Principal Supervisor | Sean Benjamin (In Progress) , Carleton University<br>Student Degree Expected Date: 2023/5<br>Thesis/Project Title: Network Control Using Distribution Based Control<br>Present Position: Master's student, Carleto University |
| 2020/9 - 2022/12<br>Co-Supervisor | Nick Perez (In Progress) , Carleton University<br>Student Degree Expected Date: 2022/12<br>Thesis/Project Title: Integrity Attacks and Replay Attacks in Quantum Networks<br>Present Position: Student, Carleton University |
| 2015/9 - 2017/5<br>Co-Supervisor | Steven Porretta (Completed) , Carleton University<br>Thesis/Project Title: Environmental Communication Optimization in Underwater Acoustic Sensor Networks<br>Present Position: PhD student at Carleton University |
| 2015/4 - 2017/4<br>Principal Supervisor | Saleh Almousa (Withdrawn) , Carleton University<br>Thesis/Project Title: Quantum Communications and Networks<br>Present Position: Work in Saudi Arabia |

**Doctorate [n=6]**

| | |
|---|---|
| 2021/1 - 2023/5<br>Academic Advisor | Mohammad T. Ramezanlou (In Progress) , Carleton University<br>Student Degree Expected Date: 2023/5<br>Thesis/Project Title: Cellular Network Controllers for Quadrotors Experiencing Time Delay<br>Present Position: PhD student at Carleton University, Carleton University |
| 2020/9 - 2024/5<br>Co-Supervisor | Banaeizadeh, Fatemeh (In Progress) , Carleton University<br>Student Degree Expected Date: 2024/9<br>Thesis/Project Title: Machine learning, drone navigation and network resource management<br>Present Position: PhD student at Carleton University, Carleton University |
| 2020/5 - 2023/5<br>Co-Supervisor | Justin Singer (In Progress) , Carleton University<br>Student Degree Expected Date: 2023/5<br>Thesis/Project Title: Quantum Reinforcement Learning through Causal Inference at the Counterfactual Level<br>Present Position: PhD student at Carleton University, Carleton University |
| 2020/1 - 2024/12<br>Principal Supervisor | Pravallika Katragunta (In Progress) , Carleton University<br>Student Degree Expected Date: 2024/12<br>Thesis/Project Title: Dynamic radio resource management and allocation for base station to drone communications<br>Present Position: PhD student at Carleton University, Carleton University |
| 2017/9 - 2022/12<br>Co-Supervisor | Steven Porretta (In Progress) , Carleton University<br>Student Degree Expected Date: 2022/12<br>Thesis/Project Title: Underwater communications and machine learning<br>Present Position: PhD student at Carleton University, Carleton University |
| 2016/9 - 2022/5<br>Principal Supervisor | Ahmad Traboulsi (Completed) , Carleton University<br>Thesis/Project Title: Quadcopter Behaviour Intention<br>Present Position: Web developper, BoatBlurp |

## Editorial Activities

| | |
|---|---|
| 2024/1 - 2024/12 | Technical Program Committee Member, IEEE ICC 2024 Quantum Communications & Information Technology Track, Book |
| 2023/1 - 2023/12 | Technical Program Committee Member, 2023 IEEE Global Communications Conference: Selected Areas in Communications: Quantum Communications and Computing, Book |
| 2023/1 - 2023/12 | Technical Program Committee Member, 2023 IEEE Interna8onal Conference on Communications; Selected Areas in Communications: Quantum Communications and Information Technology, Book |
| 2022/1 - 2022/12 | Technical Program Committee Member, 15th IEEE International Workshop on Wireless Sensor, Robot and UAV Networks (WISARN) 2022, Book |
| 2022/1 - 2022/12 | Technical Program Committee Member, 11th IEEE/CIC International Conference on Communications (ICC) 2022, Book |
| 2022/1 - 2022/12 | Technical Program Committee Member, 2022 IEEE Globecom: Quantum CommunicaWons and Information Processing, Book |
| 2022/1 - 2022/12 | Technical Program Committee Member, 17th International Conference on Risks and Security of Internet and Systems (CRISIS) 2022, Book |
| 2021/1 - 2021/12 | Technical Program Committee Member, 16th International Conference on Risks and Security of Internet and Systems (CRISIS) 2021, Book |
| 2021/1 - 2021/12 | Technical Program Committee Member, 14th IEEE International Workshop on Wireless Sensor, Robot and UAV Networks, Book |
| 2020/6 - 2021/5 | Technical Program Committee Member, 1st IEEE/IFIP International Workshop on Internet of Things Management, Book |
| 2020/6 - 2021/5 | Technical Program Committee Member, 14th IEEE International Workshop on Wireless Sensor, Robot and UAV Networks, Book |
| 2020/1 - 2020/12 | Technical Program Committee Member, Conference on Risks and Security of Internet and Systems (CRISIS) 2020, Book |
| 2019/1 - 2019/12 | Program committee member, Workshop on Quantum Communications and Information Technology (QCIT'18), at IEEE Globecom, Book |
| 2018/1 - 2018/12 | Program committee member, 2nd IEEE/IFIP International Workshop on Decentralized Orchestration and Management of Distributed Heterogeneous Things (DOMINOS), Book |
| 2017/3 - 2017/12 | Program committee member, Workshop on Quantum Communications and Information Technology (QCIT'17), at IEEE Globecom, Book |
| 2016/3 - 2017/12 | Program committee member, Workshop on Quantum Communications and Information Technology (QCIT'16), at IEEE Globecom, Book |

## Organizational Review Activities

| | |
|---|---|
| 2017/9 - 2022/6 | Member, Fonds de recherche du Québec - Santé (FRQS)<br>Evaluation and ranking of research proposals for the FNRS-FRQ Bilateral Program for Collaborative Research Québec – Communauté française de Belgique / Programme de collaboration bilatérale Québec-Fédération Wallonie-Bruxelles: |

| | |
|---|---|
| 2018/9 - 2019/6 | Evaluation committee member, Fonds de recherche du Québec - Nature et technologies (FRQNT)<br>Read and evaluation of research proposals for the program Strategic Clusters / Regroupements Stratégiques |

## Committee Memberships

| | |
|---|---|
| 2002/1 | Committee Member, Steering Committee of International Conference on Ad Hoc Networks and Wireless (AdHoc-Now), Several universities<br>Our role in this committee is to insure the sustainability and growth of the conference. |
| 2019/1 - 2019/12 | Co-chair, 12th Conference Foundations and Practice of Security, Several universities<br>General co-chair, selection of invited speakers |

## Presentations

1. (2021). Quantum-Safe and Safe Quantum Data Communications. talk.cybercni.fr – The monthly Cybersecurity Speaker Series, Rennes, France
   Main Audience: Researcher
   Invited?: Yes, Keynote?: No

## Publications

### Journal Articles

1. Kuang, R; Perepechaenko, M; *Toth, R; Barbeau, M. (2023). Performance comparisons of quantum-safe multivariate polynomial public key encapsulation algorithm. Cybersecurity. : 1-19.
   Revision Requested
   Refereed?: Yes, Open Access?: No
2. Barbeau, M. (2023). Quantum Data Communication Protection with the Quantum Permutation Pad Block Cipher in Counter Mode and Clifford Operators. F1000Research.
   Submitted
   Refereed?: Yes, Open Access?: Yes
3. Barbeau, M. (2023). Cryptographic schemes for secret long-distance underwater communications. Journal of Communications. : 1-9.
   Revision Requested
   Refereed?: Yes, Open Access?: No
4. Barbeau, M; Garcia-Alfaro, J; Kranakis, E. (2022). Research trends in collaborative drones. Sensors. 22(9): 1-17.
   Published
   Refereed?: Yes, Open Access?: Yes
5. Kuang, R; Perepechaenko, M; Barbeau, M. (2022). A new quantum-safe multivariate polynomial public key digital signature algorithm. Scientific Reports. 12: 1-21.
   Published
   Refereed?: Yes, Open Access?: Yes
6. Barbeau, M; Garcia-Alfaro, J. (2022). Cyber-physical defense in the quantum Era. Scientific Reports. 12: 1-11.
   Published
   Refereed?: Yes, Open Access?: Yes

7. Barbeau, M;Blouin, S; Traboulsi, A. (2022). Adaptable design for long range underwater communications. Wireless Networks. : 1-17.
   Published
   Refereed?: Yes, Open Access?: Yes

8. Barbeau, M; Kranakis, E; *Perez, N. (2022). Authenticity, integrity and replay protection in quantum data communications and networking. ACM Transactions on Quantum Computing. 3(2): 1-22.
   Published
   Refereed?: Yes, Open Access?: No

9. Kuang, R; Barbeau, M. (2022). Quantum permutation pad for universal quantum-safe cryptography. Quantum Information Processing. 21(211): 1-22.
   Published
   Refereed?: Yes, Open Access?: Yes

10. Kuang, R; Perepechaenko, M; Barbeau, M. (2022). A new quantum-safe multivariate polynomial public key digital signature algorithm. Scientific Reports.
    Accepted
    Refereed?: Yes, Open Access?: Yes

11. Barbeau, M; Blouin, S; Traboulsi, A. (2022). Adaptable design for long range underwater communications. Wireless Networks. : 1-17.
    Published
    Refereed?: Yes, Open Access?: Yes

12. Kuang, R; Perepechaenko, M; Barbeau, M. (2022). A new post-quantum multivariate polynomial public key encapsulation algorithm. Quantum Information Processing. 21: 1-25.
    Published
    Refereed?: Yes, Open Access?: Yes

13. Kuang, R; Barbeau, M. (2022). Quantum permutation pad for universal quantum safe cryptography. Quantum Information Processing. 21: 1-22.
    Published
    Refereed?: Yes, Open Access?: Yes

14. Barbeau, M; *Beurier, E; Garcia-Alfaro, J; Kuang, R; Pahl, M-O; Pastor, D. (2021). The quantum what? Advantage, utopia or threat?. Digital Welt (Magazine). 5(4): 34-39.
    Published
    Refereed?: Yes, Open Access?: Yes

15. Barbeau, M; Cuppens, F; Cuppens, N; *Dagnas, R; Garcia-Alfaro, J. (2021). Resilience estimation of cyber-physical systems via quantitative metrics. IEEE Access. 9: 46462-46475.
    Published
    Refereed?: Yes, Open Access?: Yes

16. *Lu; H; Barbeau, M; Nayak, A. (2019). Keyless semi-quantum point-to-point communication protocol with low resource requirements. Scientific Reports, Springer Nature Limited. 0: 1-16.
    Published
    Refereed?: Yes, Open Access?: Yes

17. Barbeau M. (2019). Protection of quantum data communications. Digitale Welt (Magazine). 3(2): 46-49.
    Published
    Refereed?: Yes, Open Access?: Yes

18. Ahmad, A-M; Barbeau, M; Garcia-Alfaro, J; *Kassem, J; Kranakis, E. (2019). Tuning the demodulation frequency based on a normalized trajectory model for mobile underwater acoustic communications. Transactions on Emerging Telecommunications Technologies. 30(12): 1-15.
    Published
    Refereed?: Yes, Open Access?: Yes

19. Barbeau, M. (2019). Recognizing drone swarm activities: Classical versus quantum machine learning. Digitale Welt (Magazine). 3(4): 45-50.
    Published
    Refereed?: Yes, Open Access?: Yes

20. Ahmad, A-M; *Kassem, J; Barbeau, M; Kranakis. E; *Porretta. S; Garcia-Alfaro, J. (2018). Doppler effect in the acoustic ultra low frequency band for wireless underwater networks. Mobile Networks and Applications (MONET), ACM Springer. : 1-11.
    Published
    Refereed?: Yes

21. Shi, W; Barbeau, M; Corriveau, J-P; Garcia-Alfaro, J; *Yao, M. (2017). Secure localization in presence of colluding attackers in WSNs. Sensors, MDPI. 17(8): 1-15.
    Published
    Refereed?: Yes

22. *Huang, J; Barbeau, M; Blouin, S; Hamm, C; Taillefer, M. (2017). Simulation and modeling of hydro acoustic communication channels with wide band attenuation and ambient noise. International Journal of Parallel, Emergent and Distributed Systems, Taylor & Francis. 32(5): 466-485.
    Published
    Refereed?: Yes

## Books

1. Benzekri, A; Barbeau, M; Gong, G; Laborde, R; Garcia-Alfaro, J. (2020). Foundations and Practice of Security. : 408.
    Published, Springer, Cham
    Refereed?: Yes

## Conference Publications

1. *Katragunta, P; Barbeau, M; Garcia-Alfaro, J; Kranakis, E. (2023). TABS Joint Optimization Serving mmWave High Altitude UAVs: A Counterfactual MAB Approach. IEEE. IEEE Global Communications Conference, Kuala Lumpur, Malaysia (1-7)
    Conference Date: 2023/12
    Paper
    Submitted
    Refereed?: Yes, Invited?: No

2. *Banaeizadeh, F; Barbeau, M; Garcia-Alfaro, J; Kranakis, E. (2023). Deep RL for UAV Trajectory Design with NOMA Uplink Interference Mitigation and Energy Consumption Minimization. IEEE. EEE Global Communications Conference, Kuala Lumpur, Malaysia (1-7)
    Conference Date: 2023/12
    Paper
    Submitted
    Refereed?: Yes, Invited?: No

3. *Porretta, S; Barbeau, M; Blouin, S; Kranakis, E; Webster, A. (2023). A Novel Underwater Packet Flooding Protocol. IEEE. 2023 Canadian Conference On Electrical and Computer Engineering, Regina, Canada (1-6)
    Conference Date: 2023/9
    Paper
    Accepted
    Refereed?: Yes, Invited?: No

4. *Burge, I; Barbeau, M; Garcia-Alfaro, J. (2023). Quantum Algorithms for Shapley Value Calculation. IEEE. IEEE Quantum Week 2023, Seattle, United States of America (1-9)
   Conference Date: 2023/9
   Paper
   Accepted
   Refereed?: Yes, Invited?: No

5. Traboulsi, A; Barbeau, M; Blouin, S. (2023). Analysis of Experimental Data Fusion Schemes for Underwater Communication over a Hydrophone Array. IEEE. 2023 Canadian Conference On Electrical and Computer Engineering, Regina, Canada (1-6)
   Conference Date: 2023/9
   Paper
   Accepted
   Refereed?: Yes, Invited?: No

6. Dagnas, R; Barbeau, M; *Boutin, M; Garcia-Alfaro, J; Yaich, R. (2023). Exploring the Quantitative Resilience Analysis of Cyber-Physical Systems. IFIP Networking Conference Proceedings. 2023 IFIP Networking Conference (IFIP Networking) - IFIP Networking 2023: IOCRCI (Impact of IT/OT Convergence on the Resilience of Critical Infrastructures), Barcelona, Spain (1-6)
   Conference Date: 2023/6
   Paper
   Accepted
   Refereed?: Yes, Invited?: No

7. Barbeau, M. (2023). Confidential Underwater Communications Using Quantum Permutation Pad in Counter Mode. ICCCAS Conference Proceedings. 12th International Conference on Communications, Circuits, and Systems (ICCCAS), Singapore, Singapore (1-6)
   Conference Date: 2023/5
   Paper
   In Press
   Refereed?: Yes, Invited?: No

8. *Beaupré, Y; Barbeau, M; Blouin, S. (2023). Underwater Confidential Communications in JANUS. Lecture Notes in Computer Science, vol 13877. Foundations and Practice of Security. FPS 2022, Ottawa, Canada (255-270)
   Conference Date: 2022/12
   Paper
   Published
   Refereed?: Yes, Invited?: No

9. Kuang, R; Perepechaenko, M; *Toth, R; Barbeau, M. (2023). Benchmark Performance of the Multivariate Polynomial Public Key Encapsulation Mechanism. Lecture Notes in Computer Science, vol 13857.Risks and Security of Internet and Systems, Sousse, Tunisia (239-255)
   Conference Date: 2022/12
   Paper
   Published
   Refereed?: Yes, Invited?: No

10. *Banaeizadeh, F; Barbeau, M; Garcia-Alfaro, J; Kothapalli, V. S.; Kranakis, E. (2022). Uplink Interference Management in Cellular-Connected UAV Networks Using Multi-Armed Bandit and NOMA. IEEE. 2022 IEEE Latin-American Conference on Communications (LATINCOM), Rio de Janeiro, Brazil (1-6)
    Conference Date: 2022/11
    Paper
    Published
    Refereed?: Yes, Invited?: No

11. Barbeau, M; Garcia-Alfaro, J; Lübben, C; Pahl, M.O.; Wüstrich, L. (2022). Resilience via Blackbox Self-Piloting Plants. CEUR Workshop Proceedings 2022 Nov 15 (Vol. 3329, No. 1). Computer & Electronics Security Application Rendezvous, co-located with the 7th European Cyber Week (ECW 2022), Rennes, France (35-46)
    Conference Date: 2022/11
    Paper
    Published
    Refereed?: Yes, Invited?: No

12. Kuang, R; Perepechaenko, M; *Toth, R; Barbeau, M. (2022). Benchmark Performance of a New Quantum Safe Multivariate Polynomial Digital Signature Algorithm. Proceedings of IEEE International Conference on Quantum Computing and Engineering (QCE22). IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, United States of America
    Conference Date: 2022/9
    Paper
    Accepted
    Refereed?: Yes, Invited?: No

13. *Tayefe Ramezanlou, M; Schwartz, H; Lambadaris, I; Barbeau, M. (2022). Comparison of Cellular Network Controllers for Quadrotors Experiencing Time Delay. Proceedings of 30th Mediterranean Conference on Control and Automation. 30th Mediterranean Conference on Control and Automation, Athens, Greece
    Conference Date: 2022/6
    Paper
    In Press
    Refereed?: Yes, Invited?: No

14. Barbeau, M; Blouin, S; Traboulsi, A. (2022). Frame Design for Adaptability in Long-Range Underwater Communication. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engi. Ad Hoc Networks and Tools for IT. ADHOCNETS 2021, Sydney, Australia (130-143)
    Conference Date: 2021/11
    Paper
    Published
    Refereed?: Yes, Invited?: No

15. Kuang, R; Barbeau, M. (2021). Indistinguishability and Non-deterministic Encryption of the Quantum Safe Multivariate Polynomial Public Key Cryptographic System. Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), (1-5)
    Paper
    Published
    Refereed?: Yes, Invited?: No

16. Kuang, R; Barbeau, M. (2021). Performance Analysis of the Quantum Safe Multivariate Polynomial Public Key Algorithm. Proceedings of IEEE International Conference on Quantum Computing and Engineering (QCE). IEEE International Conference on Quantum Computing and Engineering (QCE), Broomfield, United States of America (351-358)
    Conference Date: 2021/10
    Paper
    Published
    Refereed?: Yes, Invited?: No

17. Banaeizadeh, F; Barbeau, M; Garcia-Alfaro, J; Kranakis, E; Wan, T. (2021). Pilot Contamination Attack Detection in 5G Massive MIMO Systems Using GAN. Proceedings of IEEE International Mediterranean Conference on Communications and Networking. IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Greece (479-484)
Conference Date: 2021/9
Paper
Published
Refereed?: Yes, Invited?: No

18. Barbeau, M; Garcia-Alfaro, J; Kranakis, E. (2021). Risky Zone Avoidance Strategies for Drones. Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Canada (1-6)
Conference Date: 2021/9
Paper
Published
Refereed?: Yes, Invited?: No

19. Barbeau, M; Blouin, S; Traboulsi, A. (2021). Performance of an Underwater Communication System in a Sea Trial Done in the Canadian Arctic. Proceedings of IEEE International Mediterranean Conference on Communications and Networking. IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Greece (448-453)
Conference Date: 2021/9
Paper
Published
Refereed?: Yes, Invited?: No

20. *Traboulsi, A; Barbeau, M. (2021). A Reverse Turing Like Test for Quad-copters. Proceedings of 17th International Conference on Distributed Computing in Sensor Systems (DCOSS). 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), Coral Bay, Cyprus (351-358)
Conference Date: 2021/7
Paper
Published
Refereed?: Yes, Invited?: No

21. *Traboulsi, A; Barbeau, M. (2021). Identification of Drone Payload Using Mel-Frequency Cepstral Coefficients and LSTM Neural Networks. Advances in Intelligent Systems and Computing, vol 1288.Future Technologies Conference (FTC) 2020, Vancouver, Canada (402-412)
Conference Date: 2020/11
Paper
Published
Refereed?: Yes, Invited?: No

22. Barbeau, M; Cuppens, F ; Cuppens, N; Dagnas, R*; Garcia-Alfaro, J. (2020). Metrics to Enhance the Resilience of Cyber-Physical Systems. IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China (1167-1172)
Conference Date: 2020/12
Paper
Published
Refereed?: Yes, Invited?: No

23. Barbeau M, Garcia-Alfaro J, Kranakis E. (2020). Geocaching-inspired Navigation for Micro Aerial Vehicles with Fallible Place Recognition. Proceedings of 19th International Conference on Ad Hoc Networks and Wireless. 19th International Conference on Ad Hoc Networks and Wireless (ADHOC-NOW), Lecture Notes in Computer Science, vol 12338, Bary, Italy (55-70)
Conference Date: 2020/10
Paper
Published
Refereed?: Yes, Invited?: No

24. Barbeau, M; Garcia-Alfaro, J; Kranakis, E. (2020). Capacity Requirements of Quantum Repeaters. Proceedings of IEEE International Conference on Quantum Computing (QCE20). IEEE International Conference on Quantum Computing (QCE20), Denver, Colorado, United States of America (148-157)
Conference Date: 2020/10
Paper
Published
Refereed?: Yes, Invited?: No

25. *Traboulsi A, Barbeau M. (2019). Recognition of Drone Formation Intentions Using Supervised Machine Learning. The 2019 International Conference on Computational Science and Computational Intelligence, Las Vegas, NV, United States of America (408-411)
Conference Date: 2019/12
Paper
Published
Refereed?: Yes, Invited?: No

26. Barbeau M, Garcia-Alfaro J. (2019). Discriminating Data of a Micro Aerial Vehicle Using Quantum Generative Adversarial Networks. IEEE GLOBECOM 2019 Workshop on Quantum Communications and Information Technology, Waikoloa, HI, United States of America (1-6)
Conference Date: 2019/12
Paper
Published
Refereed?: Yes, Invited?: No

27. Barbeau, M; Garcia-Alfaro, J. (2019). Faking and Discriminating the Navigation Data of a Micro Aerial Vehicle Using Quantum Generative Adversarial Networks. IEEE. 019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, United States of America (1-6)
Conference Date: 2019/12
Paper
Published
Refereed?: Yes, Invited?: No

28. Barbeau M, Garcia-Alfaro J, Kranakis E, *Santos F. (2019). Quality Amplification of Error Prone Navigation for Swarms of Micro Aerial Vehicles. IEEE GLOBECOM 2019 Workshop on Computing-Centric Drone Networks, Waikoloa, HI, United States of America (1-6)
Conference Date: 2019/12
Paper
Published
Refereed?: Yes, Invited?: No

29. Barbeau M, Garcia-Alfaro J, Kranakis E. (2019). Geocaching-inspired Resilient Path Planning for Drone Swarms. IEEE MiSARN 2019. Joint 7th International Workshop on Mission-Oriented Wireless Sensor and Cyber-Physical System Networking (MiSeNet) and 12th International Workshop on Wireless Sensor, Robot and UAV Networks (WiSARN), co-located with INFOCOM, Paris, France (620-625)
Conference Date: 2019/4
Paper
Published
Refereed?: Yes, Invited?: No

30. Barbeau M. (2019). Secure Quantum Data Communications Using Classical Keying Material. International Workshop on Quantum Technology and Optimization Problems (QTOP), Munich, Germany (183-195)
Conference Date: 2019/3
Paper
Published
Refereed?: Yes, Invited?: No

31. Ahmad A-M, Barbeau M, Garcia-Alfaro J, *Kassem J, Kranakis E, *Porretta S. (2018). Low Frequency Mobile Communications in Underwater Networks. Ad-hoc, Mobile, and Wireless Networks. International Conference on Ad-Hoc Networks and Wireless, Saint-Malo, France (239-251)
Conference Date: 2018/9
Paper
Published
Refereed?: Yes, Invited?: No

32. *Kassem J, Barbeau M, Ahmad A.-M., Garcia-Alfaro J. (2018). The Implementation of GNU Radio Blocks for Decoding Long-lasting Frames in Mobile Underwater Acoustic Communications. The technical proceedings of the 8th Annual GNU Radio Conference. GNU Radio Conference, Henderson, NV, United States of America (1-8)
Conference Date: 2018/9
Paper
Published
Refereed?: Yes, Invited?: No

33. *Kassem J, Barbeau M, Ahmad A.-M., Garcia-Alfaro J. (2018). GNU Radio Blocks for Long-lasting Frames in Mobile Underwater Acoustic Communications. French GNU Radio Days. French GNU Radio Days 2018, Lyon, France (1-2)
Conference Date: 2018/7
Abstract
Published
Refereed?: Yes, Invited?: No

34. *Lu H, Barbeau M, Nayak A. (2018). Economic No-Key Semi-Quantum Direct Communication Protocol. 2017 IEEE Globecom Workshops (GC Wkshps). Quantum Communications and Information Technology (QCIT'17), Singapore, Singapore (1-7)
Conference Date: 2017/12
Paper
Published
Refereed?: Yes, Invited?: No

35. Ahmad A-M, Barbeau M, Garcia-Alfaro J, *Kassem J, Kranakis E, *Porretta S. (2018). Doppler Effect in the Underwater Acoustic Ultra Low Frequency Band. Ad Hoc Networks, Springer International Publishing. Proceedings of the 9th EAI International Conference on Ad Hoc Networks, Niagara Falls, Canada (3-12)
Conference Date: 2017/9
Paper
Published
Refereed?: Yes, Invited?: No

36. Barbeau M, Garcia-Alfaro J, Kranakis E, *Porretta S. (2018). The Sound of Communication in Underwater Acoustic Sensor Networks. Ad Hoc Networks, Springer International Publishing. 9th International Conference, AdHocNets 2017, Niagara Falls, Canada (13-23)
Conference Date: 2017/9
Paper
Published
Refereed?: Yes, Invited?: No

37. *Porretta S, Garcia-Alfaro J, Barbeau M, Kranakis E. (2017). Learning to communicate underwater: An exploration of limited mobility agents. WUWNET 2017, Association for Computing Machinery, Inc. International Conference on Underwater Networks and Systems, Halifax, Canada (1-5)
Conference Date: 2017/11
Paper
Published
Refereed?: Yes, Invited?: No

38. Barbeau M. (2017). Weak Signal Underwater Communications in the Ultra Low Frequency Band. 7th GNU Radio Conference. 7th GNU Radio Conference, Las Vegas, United States of America (1-8)
Conference Date: 2017/9
Paper
Published
Refereed?: Yes, Invited?: No

39. Blouin S, Barbeau M. (2017). An Experimental Baseline for Underwater Acoustic Broadcasts. IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, Canada (1-5)
Conference Date: 2017/9
Paper
Published
Refereed?: Yes, Invited?: No

40. Barbeau M, *Renaud Z, *Wang W. (2017). Management of surveillance underwater acoustic networks. 8th International Conference, ADHOCNETS 2016, Ottawa, Canada (3-14)
Conference Date: 2016/9
Paper
Published
Refereed?: Yes, Invited?: Yes

# David Barrera

*Assistant Professor, Carleton University*

*david.barrera@carleton.ca*
*https://dbarrera.xyz*
*He/Him/His*
*English, Français, Español*

## Impact Summary

- Early career researcher with 1900+ citations and h-index of 17.
- Significant contributions in the areas of: secure software installation, Internet of Things security, anonymous communication on future internet architectures, and cybersecurity practices in emergency departments.
- Publications in top tier computer security conferences (ACM CCS, ACM CHI, IEEE Euro S&P, Financial Cryptography, ACSAC) and journals (ACM TOPS, Communications of the ACM, IEEE Security and Privacy Magazine).

## Career Experience

July 2019– **Assistant Professor**, *Carleton University*, Ottawa, Canada
School of Computer Science

2017–2019 **Assistant Professor**, *Polytechnique Montréal*, Quebec, Canada
Department of Software and Computer Engineering

2016–2017 **Visiting Scientist**, *IBM Research Zürich*, Switzerland
Member of the information security group.

2014–2016 **Postdoc**, *ETH Zürich*, Switzerland
Researcher in the Network Security Group. Advisor: Dr. Adrian Perrig.

## Education

2010–2014 **PhD, Computer Science**, *Carleton University*, Ottawa, Canada
Thesis title: Securing Decentralized Software Installation and Updates.
Supervisor: Dr. Paul C. van Oorschot (Carleton University).
Committee: Dr. Robert Biddle (Carleton University), Dr. Ashraf Matrawy (Carleton University), Dr. Guy-Vincent Jourdan (University of Ottawa), Dr. Aviel Rubin (Johns Hopkins University).

2007–2009 **Master of Computer Science**, *Carleton University*, Ottawa, Canada
Thesis title: Towards Classifying and Selecting Appropriate Security Visualization Techniques.

2006–2007 **Post-graduate Diploma in Information Systems Security**, *Tecnológico de Monterrey*, Mexico City, Mexico

2002–2006 **Bachelor of Science (Honours) in Electronic Systems Engineering**, *Tecnológico de Monterrey*, Mexico City, Mexico

## Professional Leaves

2021 Parental leave. 4 months (September-December) of joint parental leave with my partner to care for our newborn son. My supervised students continued their research independently, or jointly with other members of the department through co-supervisions, but no manuscripts were submitted for peer-review during this period.

2018 Parental leave. 5 months (August-December) of parental leave as the primary caregiver for our 6 month old daughter. My supervised students continued research with their co-supervisors, but no manuscripts were submitted for peer-review during this period.

## Funding

| | | |
|---|---|---|
| 2023 | SSHRC HC2P Partnership Grant | *CAD$10,000* |
| 2018 | NSERC Discovery Launch Supplement | *CAD$12,500* |
| 2018–2023 | NSERC Discovery Grant (Early Career Researcher) | *CAD$23,000/year* |
| 2017–2022 | MIWF Förderlinie "Digitale Sicherheit" (Germany) – Declined | *€ 600,000* |
| 2011–2014 | NSERC Canada Graduate Scholarship (CGS D3) | *CAD$35,000/year* |
| 2011–2014 | School of Computer Science Departmental Scholarship | *CAD$1,700/year* |
| 2008–2009 | Ontario Graduate Scholarship in Science and Technology | *CAD$15,000/year* |
| 2008–2009 | J. James Mackie Endowment for Graduate Scholarships in Human-Technology Interaction | *CAD$3,000/year* |
| 2006 | Academic Scholarship | *CAD$10,000/year* |

## Most Cited Publications

1. *715 citations* - **A Methodology for Empirical Analysis of Permission-based Security Models and its Application to Android**. David Barrera, H.G. Kayacik, P.C. van Oorschot, and Anil Somayaji. In Proceedings of the ACM Conference on Computer and Communications Security (CCS). 2010.
2. *203 citations* - **A First Look at the Usability of Bitcoin Key Management**. Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. In Proceedings of the NDSS Workshop on Usable Security (USEC). 2015.
3. *145 citations* - **HORNET: High-speed Onion Routing at the Network Layer**. Chen Chen, Daniele E. Asoni, David Barrera, George Danezis, and Adrian Perrig. In Proceedings of the ACM Conference on Computer and Communications Security (CCS). 2015.
4. *113 citations* - **Secure Software Installation on Smartphones**. David Barrera and P.C. van Oorschot. IEEE Security & Privacy Magazine, 9(3):42–48, May 2011.
5. *98 citations* - **Understanding and Improving App Installation Security Mechanisms through Empirical Analysis of Android**. David Barrera, Jeremy Clark, Daniel McCarney, and P.C. van Oorschot. In Proceedings of the Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM). 2012.

## Refereed Journals and Periodicals

2023 **IoT Security Best Practices: A Critical Analysis**. David Barrera, Christopher Bellman, and P.C. van Oorschot. *ACM Transactions on Privacy and Security*, 26(2):13:1–13:30, 2023.

**A Close Look at a Systematic Method for Analyzing Sets of Security Advice**. David Barrera, Christopher Bellman, and P.C. van Oorschot. *Journal of Cybersecurity*, 2023. Oxford University Press. To appear. Accepted May 18, 2023.

2021 **The EDIT Survey: Identifying Emergency Department Information Technology Knowledge and Training Gaps**. Daniel Kollek, David Barrera, Elizabeth Stobert, and Valerie Homier. *Journal of Disaster Medicine and Public Health Preparedness*, pages 1–6, 2021. Cambridge University Press.

2017 **The SCION Internet Architecture**. David Barrera, Laurent Chuat, Adrian Perrig, Raphael M. Reischuk, and Pawel Szalachowski. *Communications of the ACM*, 60(6):56–65, May 2017.

2011 **Back to the Future: Revisiting IPv6 Privacy Extensions**. David Barrera, Glenn Wurster, and P.C. van Oorschot. *;LOGIN: The USENIX Magazine*, 36(1):16–26, 2011.

**Secure Software Installation on Smartphones**. David Barrera and P.C. van Oorschot. *IEEE Security & Privacy Magazine*, 9(3):42–48, May 2011.

2010 **Accommodating IPv6 Addresses in Security Visualization Tools**. David Barrera and P.C. van Oorschot. *SAGE Information Visualization*, 10(2):107–116, 2010.

## Refereed Conference and Workshop Papers

2023 **If-This-Then-Allow-That (to Phone Home): A Trigger-Based Network Policy Enforcement Framework for Smart Homes**. Anthony Tam, Furkan Alaca, and David Barrera. In Guy-Vincent Jourdan, Laurent Mounier, Carlisle Adams, Florence Sèdes, and Joaquin Garcia-Alfaro, editors, *Foundations and Practice of Security*, pages 373–388. Springer Nature Switzerland, April 2023. 37% acceptance rate.

**Towards Characterizing IoT Software Update Practices**. Conner Bradley and David Barrera. In Guy-Vincent Jourdan, Laurent Mounier, Carlisle Adams, Florence Sèdes, and Joaquin Garcia-Alfaro, editors, *Foundations and Practice of Security*, pages 406–422. Springer Nature Switzerland, April 2023. 37% acceptance rate. Runner up for best paper award.

2020 **SERENIoT: Collaborative Network Security Policy Management and Enforcement for Smart Homes**. Corentin Thomasset and David Barrera. In *Annual Computer Security Applications Conference (ACSAC)*, pages 542–555, 2020. 23% acceptance rate.

**Understanding Cybersecurity Practices in Emergency Departments**. Elizabeth Stobert, David Barrera, Valérie Homier, and Daniel Kollek. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI'20, pages 1–8. ACM, 2020. 24% acceptance rate.

**bpfbox: Simple Precise Process Confinement with eBPF**. William Findlay, Anil Somayaji, and David Barrera. In *ACM Cloud Computing Security Workshop (CCSW)*, 2020. 13 pages. 30% acceptance rate.

2018 **TARANET: Traffic-Analysis Resistant Anonymity at the NETwork layer**. Chen Chen, Daniele E. Asoni, Adrian Perrig, David Barrera, George Danezis, and Carmela Troncoso. In *Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 137–152, 2018. 22% acceptance rate.

**Standardizing IoT Network Security Policy Enforcement**. David Barrera, Ian Molloy, and Heqing Huang. In *Proceedings of the NDSS Workshop on Decentralized IoT Security and Standards (DISS)*, 2018. 6 pages. 41% acceptance rate.

2017 **Internet Kill Switches Demystified**. Benjamin Rothenberger, Daniele E. Asoni, David Barrera, and Adrian Perrig. In *Proceedings of the 10th European Workshop on Systems Security*, EuroSec'17, pages 1–6. ACM, April 2017. 37% acceptance rate.

2016 **Picking a (Smart)Lock: Locking Relationships on Mobile Devices (short paper)**. Elizabeth Stobert and David Barrera. In *Proceedings of Who Are You?!: Adventures in Authentication Workshop (WAY)*, June 2016. 2 pages. Extended abstract.

**Source Accountability with Domain-brokered Privacy**. Taeho Lee, Christos Pappas, David Barrera, Pawel Szalachowski, and Adrian Perrig. In *Proceedings of the ACM Conference on Emerging Networking Experiments and Technologies (CoNEXT)*, pages 345–358. ACM, December 2016. 18% acceptance rate.

**Modeling Data-Plane Power Consumption of Future Internet Architectures**. Chen Chen, David Barrera, and Adrian Perrig. In *Proceedings of the IEEE Conference on Collaboration and Internet Computing (CIC)*, pages 149–158, November 2016.

2015 **A First Look at the Usability of Bitcoin Key Management**. Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. In *Proceedings of the NDSS Workshop on Usable Security (USEC)*, February 2015. 38% acceptance rate.

**HORNET: High-speed Onion Routing at the Network Layer**. Chen Chen, Daniele E. Asoni, David Barrera, George Danezis, and Adrian Perrig. In *Proceedings of the Conference on Computer and Communications Security (CCS)*, pages 1441–1454. ACM, 2015. 19% acceptance rate.

**On Building Onion Routing into Future Internet Architectures**. Daniele E. Asoni, Chen Chen, David Barrera, and Adrian Perrig. In Dogan Kesdogan and Jan Camenisch, editors, *IFIP WG 11.4 International Workshop (iNetSec). Revised Selected Papers*, Open Problems in Network Security, pages 71–81. Springer LNCS vol. 9591, October 2015.

**What Lies Beneath? Analyzing Automated SSH Bruteforce Attacks**. AbdelRahman Abdou, David Barrera, and Paul C. van Oorschot. In *Proceedings of the International Conference on Passwords*, pages 72–91. Springer LNCS vol. 9551, 2015. Presenter, 33% acceptance rate.

2014 **Baton: Certificate Agility for Android's Decentralized Signing Infrastructure**. David Barrera, Daniel McCarney, Jeremy Clark, and P.C. van Oorschot. In *Proceedings of the Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, pages 1–12. ACM, 2014. Presenter, 26% acceptance rate.

2013 **Deadbolt: Locking Down Android Encryption**. Adam Skillen, David Barrera, and P.C. van Oorschot. In *Proceedings of the Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, pages 3–14. ACM, November 2013. 24% acceptance rate.

2012 **Tapas: Design, Implementation, and Usability Evaluation of a Password Manager**. Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and P.C. van Oorschot. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 89–98. ACM, December 2012. 19% acceptance rate.

**ThinAV: Truly Lightweight Mobile Cloud-based Anti-malware**. Chris Jarabek, David Barrera, and John Aycock. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 209–218. ACM, December 2012. 19% acceptance rate.

**Meteor: Seeding a Security-Enhancing Infrastructure for Multi-market Application Ecosystems**. David Barrera, William Enck, and P.C. van Oorschot. In *Proceedings of the Mobile Security Technologies Workshop (MoST)*. IEEE, May 2012. 10 pages. Presenter, 39% acceptance rate.

**Understanding and Improving App Installation Security Mechanisms through Empirical Analysis of Android**. David Barrera, Jeremy Clark, Daniel McCarney, and P.C. van Oorschot. In *Proceedings of the Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, pages 81–92. ACM, October 2012. Presenter, 36% acceptance rate.

2011 **Mercury: Recovering Forgotten Passwords Using Personal Devices**. Mohammad Mannan, David Barrera, Carson Brown, David Lie, and P.C. van Oorschot. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*, pages 315–330. Springer, 2011. 35% acceptance rate.

2010 **A Methodology for Empirical Analysis of Permission-based Security Models and its Application to Android**. David Barrera, H.G. Kayacik, P.C. van Oorschot, and Anil Somayaji. In *Proceedings of the Conference on Computer and Communications Security (CCS)*, pages 73–84. ACM, October 2010. Presenter, 17% acceptance rate.

2009 **FiGD: An Open Source Intellectual Property Violation Detector**. Carson Brown, David Barrera, and Dwight Deugo. In *Proceedings of the International Conference on Software Engineering and Knowledge Engineering (SEKE)*, pages 536–541, July 2009. 38% acceptance rate.

**Security Visualization Tools and IPv6 Addresses**. David Barrera and P.C. van Oorschot. In *Proceedings of the International Workshop on Visualization for Cyber Security (VizSec)*, pages 21–26, 2009. Presenter, 43% acceptance rate.

2008 **Improving Security Visualization with Exposure Map Filtering**. Mansour Alsaleh, David Barrera, and P.C. van Oorschot. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 205–214. ACM, December 2008. Presenter, 24% acceptance rate.

## Book Chapters

2017 **Security Analysis**. David Barrera, Tobias Klenze, Adrian Perrig, Raphael M. Reischuk, Benjamin Rothenberger, and Pawel Szalachowski. In *SCION: A Secure Internet Architecture*, chapter 13, pages 319–351. Springer International Publishing, 2017.

**The SCION Architecture**. David Barrera, Laurent Chuat, Adrian Perrig, Raphael M. Reischuk, and Pawel Szalachowski. In *SCION: A Secure Internet Architecture*, chapter 2, pages 17–45. Springer International Publishing, 2017.

**Introduction**. David Barrera, Laurent Chuat, Adrian Perrig, Raphael M. Reischuk, and Pawel Szalachowski. In *SCION: A Secure Internet Architecture*, chapter 1, pages 1–16. Springer International Publishing, 2017.

**Power Consumption**. David Barrera, Chen Chen, and Adrian Perrig. In *SCION: A Secure Internet Architecture*, chapter 14, pages 353–360. Springer International Publishing, 2017.

## Technical Reports

2022 **Ontology-Based Anomaly Detection for Air Traffic Control Systems**. Christopher Neal, Jean-Yves de Miceli, David Barrera, and José M. Fernandez. *arXiv/2207.00637*, 2022. 14 pages.

2021 **BPFContain: Fixing the Soft Underbelly of Container Security**. William Findlay, David Barrera, and Anil Somayaji. *arXiv/2102.06972*, 2021. 16 pages.

2015 **Bootstrapping Real-world Deployment of Future Internet Architectures**. Tae-Ho Lee, Pawel Szalachowski, David Barrera, Adrian Perrig, Heejo Lee, and David Watrin. *arXiv/1508.02240*, August 2015. 13 pages.

## Theses

2014 David Barrera. *Securing Decentralized Software Installation and Updates*. PhD thesis, Carleton University, 2014.

2009 David Barrera. Towards Classifying and Selecting Appropriate Security Visualization Techniques. Master's thesis, Carleton University, 2009.

## Student Supervision

With the exception of students denoted with (*) below, I have acted as the primary supervisor, mentoring students throughout their degrees. Co-supervisions were required for several reasons: (1) my position at ETH Zürich did not allow independent supervisions; (2) my move from Polytechnique Montréal to Carleton would have impacted students' abilities to complete their degrees; and (3) to ensure students were supported during my parental leaves.

### Current Students

2022 **Anastasiya Andrushchak**, *Master's Thesis*, Carleton University, Topic TBD (expected Summer 2025)

2021 **Conner Bradley**, *Master's Thesis*, Carleton University, Extending IoT Device Longevity (expected Summer 2023)

2018 **Arghavan Moradi***, *Co-supervised PhD*, Polytechnique Montréal, Topic TBD (expected Fall 2023)

### Alumni

2021 **William Findlay***, *Co-supervised Master's Thesis*, Carleton University, A Practical, Lightweight, and Flexible Confinement Framework in eBPF

2021 **Itzael Jimenez Aranda**, *Co-supervised Master's Thesis*, Polytechnique Montréal, Towards Improving the Security and Privacy of Discovery Protocols in IoT

2020 **Basma Chandid**, *Co-supervised Master's Thesis*, Polytechnique Montréal, Empirical Use of Network Time Protocol in Internet of Things Devices: Vulnerabilities and Security Measures

2020 **Corentin Thomasset**, *Co-supervised Master's Thesis*, Polytechnique Montréal, SERENIoT: Distributed Network Security Policy Management and Enforcement for Smart Homes

2017 **Marwen Jadla**, *Co-supervised Master's Thesis*, Polytechnique Montréal, Using Trusted Hardware to Secure Authentication

2016 **Pedro Mendez Montejano**, *Co-supervised Master's Thesis*, ETH Zürich, Automated Risk Score for Large-Scaled Network Intrusion Detection
Thesis supervised in collaboration with Open Systems AG.

2016 **Xuan Cai**, *Co-supervised Master's Thesis*, ETH Zürich, Anonymity Systems for Corporate Customers
Thesis supervised in collaboration with Swisscom AG.

2016 **Benjamin Rothenberger**, *Co-supervised Master's Thesis*, ETH Zürich, Towards Automated Vulnerability Discovery on Future Internet Architectures

2015 **Oliver Richter et al.**, *Co-supervised Bachelor's Group Project*, ETH Zürich, Tasky: Intelligent Calendar Event Scheduling

2015 **Daniele E. Asoni**, *Co-supervised Master's Thesis*, ETH Zürich, Secure High-Speed Anonymity Systems on Future Internet Architectures
Thesis awarded the 2015 ETH Medal and the Information Security Society of Switzerland (ISSS) Excellence Award

2015 **Lionel Bruchez**, *Co-supervised Master's Thesis*, ETH Zürich, Highly Available and Reliable Name and Path Lookups in Future Internet Architectures

2011 **Michelle Burrows**, *Dean's Summer Research Internship (DSRI) Mentor*, Carleton University

## Academic Service

### Technical Program Committee Member

2023 USENIX Security Symposium (PC vice-chair), IEEE Security and Privacy, Symposium on Foundations & Practice of Security, ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)

2022 USENIX Security Symposium, ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), USENIX Workshop on Cyber Security Experimentation and Test (CSET)

2021 ACM Computer and Communications Security (CCS), USENIX Security Symposium, USENIX Workshop on Cyber Security Experimentation and Test (CSET), ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)

2020 USENIX Workshop on Cyber Security Experimentation and Test (CSET), IEEE Workshop on the Internet of Safe Things (SafeThings), EAI International Conference on Security and Privacy in Communication Networks (SecureComm 20)

2019 Who are you? Adventures in Authentication Workshop (WAY), ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)

2018 USENIX Security Symposium, ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), ACM CCS Posters (co-chair)

2017 Network and Distributed System Security Symposium (NDSS), ACM Asia Conference on Computer and Communications Security (ASIACCS), Conference on emerging Networking EXperiments and Technologies (CoNEXT), IEEE Security and Privacy Workshop on Mobile Security Technologies (MoST), ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Innovations in Mobile Privacy and Security (IMPS)

2016 ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), ACM CCS Posters, IEEE Security and Privacy Workshop on Mobile Security Technologies (MoST), Who are you? Adventures in Authentication Workshop (WAY), Innovations in Mobile Privacy and Security (IMPS)

2015 ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)

2014 ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Annual Computer Security Applications Conference (ACSAC), IEEE Symposium on Visualization for Cyber Security (VizSec), ACM CHI Workshop on Inconspicuous Interaction

2013 Annual Computer Security Applications Conference (ACSAC), ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), IEEE Symposium on Visualization for Cyber Security (VizSec)

2012 IEEE Symposium on Visualization for Cyber Security (VizSec)

2011 IEEE Symposium on Visualization for Cyber Security (VizSec)

2010 IEEE Symposium on Visualization for Cyber Security (VizSec)

### Journal Reviewer

2022 International Journal of Health Policy and Management (IJHPM)

2013–2015, 2022 IEEE Transactions on Dependable and Secure Computing (TDSC)

2020 IEEE Internet of Things Journal

2014,2018 Elsevier Computers and Security

2010, 2015, 2017, 2018 IEEE Security & Privacy Magazine

2015–2016 De Gruyter Proceedings on Privacy Enhancing Technologies (PoPETs)

2015 IEEE Transactions on Mobile Computing (TMC)

2012 IEEE Computer

### Grant Reviewing

2019, 2022 External reviewer for the NSERC Discovery Grants Program

2022 Extternal reviewer for the MITACS Accelerate program

2020–2021 Reviewer for the FRQNT Research Support for New Academics Grants Program

2019 External reviewer for the Dutch Research Council (NWO) Cyber Security, Digital Security & Privacy Grants Program

2019 External reviewer for the NSERC Collaborative Research and Development or Industrial Research Chair Program

### Conference Organization

2023 Usenix Security Program Committee Vice-Chair, Anaheim, CA, USA

2022,2023 Artifact evaluation co-chair at ACM WiSec

October 2018 Poster session co-chair at the ACM Conference on Computer and Communications Security (CCS), Toronto, Canada

July 2013 Co-organizer of the NSERC ISSNet Student Day, University of Calgary, Canada

## Awards and Nominations

2019 Awarded the Meritas teaching award in the category of "Best professor in the department of computer and software engineering" at Polytechnique Montréal. See description of the award below.

2017 Nominated for the Meritas teaching award in the category of "Best professor in the department of computer and software engineering" at Polytechnique Montréal. The selection process is organized by the undergraduate student association, who solicit votes from the student body for best professors in their program.

## Software Development

**SCION on Mininet.** Developed the SCION integration for Mininet, a network emulation tool. This integration allowed for rapid prototyping and simulation during the early stages of SCION development at ETH Zürich, which allowed the research group to test complex topologies and scenarios without needing physical hardware. SCION on Mininet was instrumental in the larger build out of the codebase and overall architecture.

**Android Observatory.** Co-developed and maintained the Android Observatory, which indexed over 10k user-submitted Android applications. The Observatory was designed to accept user-submitted Android applications and analyze their digital signature data to provide insights into the application's potential origin and trustworthiness. The Observatory saw active use by industry and academic communities, with some scientific publications using Android Observatory URLs as canonical references to analyzed applications.

**IPv6 Privacy Extensions.** Co-developed an IPv6 privacy extension algorithm that prevents tracking users across networks. The algorithm and Linux kernel patch were not directly merged, but in 2014 appeared as an independently published IETF RFC (RFC7217). The RFC is essentially the same idea we co-developed in 2011, and it is now the default mechanism to generate private IPv6 addresses in the majority of Linux distributions, and modern Windows, macOS, Android, and iOS releases.

## Teaching Experience

Winter 2023 **IoT Security**, *Carleton University*, Canada
COMP5119. 6 students.

Winter 2023 **Computer Systems Security**, *Carleton University*, Canada
COMP4108. 62 students.

Fall 2022 **Applied Cryptography and Authentication**, *Carleton University*, Canada
COMP3109. 120 students.

Winter 2022 **IoT Security**, *Carleton University*, Canada
COMP5119. 10 students.

Winter 2022 **Computer Systems Security**, *Carleton University*, Canada
COMP4108. 36 students.

Winter 2021 **Applied Cryptography**, *Carleton University*, Canada
COMP4109. 60 students.

Winter 2021 **Operating Systems Security**, *Carleton University*, Canada
COMP5900T. 10 students.

Fall 2020 **Distributed Operating Systems**, *Carleton University*, Canada
COMP4000. 30 students.

Fall 2020 **Operating Systems Security**, *Carleton University*, Canada
COMP5900T. 19 students.

Winter 2019 **Operating Systems Security**, *Polytechnique Montréal*, Canada
INF6953K. 10 students.

Winter 2019 **Information Security**, *Polytechnique Montréal*, Canada
INF4420a. 112 students. Awarded Meritas teaching award.

Fall 2018 **Information Security**, *Polytechnique Montréal*, Canada
INF4420a. 95 students.

Fall 2017 **Information Security**, *Polytechnique Montréal*, Canada
INF4420a. 47 students. Nominated for Meritas teaching award.

2015–2016 **Teaching assistant**, *ETH Zürich*, Switzerland
Designed and graded assignments for the Operating Systems and Networking course (undergraduate). Ran tutorials discussing these assignments.

2014–2015 **Guest lecturer**, *ETH Zürich*, Switzerland
Systems security (graduate) covering Android, Linux/SELinux, and secure operating systems. Network security (graduate) covering foundations of networking and IPv6.

2014 **Guest lecturer**, *Carleton University*, Ottawa, ON, Canada
Computer Systems Security (undergraduate) covering secure software installation and network firewalls.

Jul 2010 **Co-instructor, Workshop on Smartphone Security**, *University of British Columbia*, Vancouver, B.C., Canada
Presented a history and threat analysis of smartphones. Also covered a detailed security analysis of the Blackberry, Android, Apple iOS, and Meego operating systems including hands-on labs. The workshop was part of the annual NSERC ISSNet Summer School on topics related to network security, systems security, human-oriented security.

2007–2009 **Teaching assistant**, *Carleton University*, Ottawa, Canada
Developed and ran tutorials and held office hours for undergraduate Computer Science courses (Computer Organization, Object Oriented Programming and Operating Systems)

## Invited Talks

June 2021 **Concordia University**, Montreal, QC, Host: Dr. Mohammad Mannan
SERENIoT: Distributed Network Security Policy Management and Enforcement for Smart Homes

Nov 2018 **Carleton University**, Ottawa, ON, Host: Dr. Paul van Oorschot
IoT Security Research: Trends and Directions

Dec 2017 **McMaster University**, Hamilton, ON, Host: Dr. Ridha Khedri
Security and Privacy in Future Internet Architectures

Dec 2016 **UBS Security Champions**, Zürich, Switzerland
Introduction to Android Security

Jul 2016 **UBS Security Champions**, Zürich, Switzerland
Future Internet Architectures

Apr 2016 **IBM Research Zürich**, Zürich, Switzerland, Host: Andreas Wespi
Security and Privacy in Future Internet Architectures

Apr 2016 **ETH Meets California at IBM**, San Jose, USA
The SCION Future Internet Architecture

Apr 2016 **IBM T.J. Watson**, NY, USA, Host: Dr. Ian Molloy
Security and Privacy in Future Internet Architectures

Mar 2016 **University of New Brunswick**, Fredericton, N.B., Canada, Host: Dr. Ali Ghorbani
Security and Privacy in Future Internet Architectures

Mar 2014 **University of Edinburgh**, UK, Host: Dr. David Aspinall
Baton: Certificate Agility for Android's Decentralized Signing Infrastructure

Aug 2013 **University of New Brunswick**, Fredericton, N.B., Canada, Host: Dr. Natalia Stakhanova
Key Agility for Android without a Centralized Certificate Infrastructure

Aug 2012 **Concordia University**, Montreal, QC, Canada, Host: Dr. Mohammad Mannan
Design and Implementation of the Android Observatory

Aug 2011 **Nokia Research Center**, Palo Alto, CA, USA, Host: Dr. Cynthia Kuo
Addressing Security in Multi-market Application Ecosystems

Feb 2011 **University of Ottawa**, Ontario, Canada, Host: Dr. Guy-Vincent Jourdan
Security of Android Software Installation

Dec 2010 **University of Toronto**, Ontario, Canada, Host: Dr. Mohammad Mannan
A Methodology for Empirical Analysis of Permission-based Security Models and its Application to Android

Nov 2010 **SIGCHI Ottawa Chapter (CapCHI)**, Ottawa, ON, Canada, Host: Dr. Robert Biddle
Usability and Security of Android, Google's Open Source Smartphone System

Aug 2010 **Dalhousie University**, Halifax, NS, Canada, Host: Dr. Nur Zincir-Heywood
Android OS Security Architecture

## Other Presentations

Aug 2018 **USENIX Security**, Baltimore, MD, USA
Poster: Analyzing TLS Use on IoT Devices

Aug 2013 **USENIX Security**, Washington D.C, USA
Poster: Baton for Android: Key Agility without a Centralized Certificate Infrastructure

Aug 2012 **USENIX Security**, Bellevue, WA, USA
Rump session talk: Bypassing Android's Liveness Detection with Facebook. Posted to YouTube with 67,000+ views (`youtube.com/watch?v=zYxphDK6s3I`)

Oct 2011 **CCS SPSM**, Chicago, USA
Panelist: Security implications of Android: a "closed system, open software" Mobile Platform

Dec 2010 **Research In Motion (RIM) Research Day**, Waterloo, ON, Canada
Poster: Continuum of Software Installation Models on Smartphones

Aug 2010 **USENIX Security**, Washington DC, USA
Rump session talk: A Methodology for Analyzing Permission-Based Security Models

Aug 2008 **USENIX Security**, San Jose, CA, USA
Poster: Improving Security Visualization with Exposure Map Filtering

# Curriculum Vitae of Robert Biddle, May 2023

robert.biddle@carleton.ca

1. NAME and POSITION:
   Robert Lewis Biddle
   Professor, School of Computer Science and Department of Cognitive Science
   Carleton University, Ottawa, Canada

2. DEGREES:

   - Dip.Ed., University of Otago, Education, 1988.
   - Ph.D., University of Canterbury, Computer Science, 1986.
   - M.Math., University of Waterloo, Computer Science, 1979.
   - B.Math. (Hons. Co-op.), University of Waterloo, Computer Science, 1977.

3. EMPLOYMENT HISTORY:

   - 2021-, Honourary Academic Appointment, School of Computer Science University of Auckland, Auckland, New Zealand
   - 2010-, Full Professor, School of Computer Science, Cross-Appointed to Institute of Cognitive Science, Carleton University, Ottawa. *(Founder and Director, HCI Graduate Program; Member, Research Ethics Committee; Member Tenure and Promotions Committee)*
   - 2004-2010, Full Professor, Office of the Dean, Faculty of Arts and Social Sciences, Carleton University, Ottawa. *(Secretary, FASS Faculty Board)*
   - 2000-2003, Reader, School of Mathematical and Computing Sciences, Cross-Appointed to School of Information Management, Victoria University of Wellington, New Zealand. *(Director, Computer Science Undergraduate Program, Chair; Science Workloads and Assessment Committee)*
   - 1995-2000, Senior Lecturer, School of Mathematical and Computing Sciences, Victoria University of Wellington, New Zealand. *(Director, Computer Science Undergraduate Program; Chair, Science Workloads and Assessment Committee)*
   - 1990-1995, Lecturer, Department of Computer Science, Victoria University of Wellington, New Zealand.
   - 1986-1988, Lecturer, Department of Computer Science, University of Canterbury, New Zealand.
   - 1979-1980, Software Researcher, Bell Northern Research, Toronto.

4. ACADEMIC HONOURS:

   - 2023: Invited Keynote Speaker, New Zealand Cybersecurity Conference
   - 2021: Invited Keynote Speaker, ACM History of Programming Languages
   - 2021: Invited Inaugural Speaker, Software Innovation New Zealand
   - 2020: Invited Keynote Speaker, Advanced Studies Program, Brugg, Switzerland
   - 2019: Invited Keynote Speaker, Pattern Languages of Programming, Ottawa
   - 2019: Invited Keynote Speaker, International Workshop on Cooperative and Human Aspects of Software Engineering, Montreal

- 2019: Invited Keynote Speaker, International Conference on Agile Software Development, Montreal
- 2019: Carleton University Graduate Mentoring Award
- 2017: Invited Keynote Speaker, Symposium on Social Technical Systems for Security, Orlando
- 2016: Outstanding Paper, Journal of Information Management and Computer Security
- 2016: Invited Speaker, EU Visual Analytics Spring School, London
- 2016: Invited Speaker, Software Engineering Programme, Oxford
- 2016: Invited Speaker, OOP Conference, Munich, Germany
- 2015: Best Paper, Cambridge Authentication Symposium
- 2015: Invited Keynote Speaker, Security Requirements Workshop, Ottawa
- 2014: Invited Keynote Speaker, Psychology of Programming Conference, Brighton
- 2014: Invited Keynote Speaker, OOP Conference, Munich
- 2012: Co-Author, Honorable Mention for Best Paper, ACM Computer-Supported Collaborative Work
- 2010: Supervisor, Bronze Medalist, ACM SIGCHI Undergraduate Student Research Competition
- 2010: Nomination, TV Ontario Best Lecturer
- 2007: Co-Author, Best Paper, Symposium on Usable Privacy and Security
- 2006: Co-author, Top Ten Game Studies Paper
- 2003: Co-supervisor, Silver Medalist, ACM Undergraduate Student Research Competition
- 2002: Finalist, NZ Prime Minister's Tertiary Teaching Excellence Award
- 2002: Victoria Univ. Award for Teaching Excellence
- 2000: Elected Fellow of New Zealand Computer Society
- 1996: Victoria Univ. Award for Special Academic Achievement
- 1981: British Commonwealth Scholar

5. SCHOLARLY and PROFESSIONAL ACADEMIC ACTIVITIES:

Past seven years: program and appointment reviews

- 2021: Ontario Tech University, Promotion to Full Professor
- 2021: University of Waterloo, Promotion to Full Professor
- 2018: University of Waterloo, Tenure Approval
- 2018: Rutgers University, Tenure Approval
- 2018:Carnegie-Mellon University, PhD External Examiner
- 2018: University of Ontario Institute of Technology, PhD External Examiner
- 2016, University of Ontario Institute of Technology, Promotion to Full Professor
- 2016, University of British Columbia, Promotion to Full Professor
- 2015 Royal Military College, Promotion to Associate Professor
- 2014 University of Western Ontario, Promotion to Full Professor
- 2014 University of Waterloo, Tenure Approval
- 2014 University of Regina, Promotion to Full Professor

Past seven years: board positions

- 2017–current Tutte Institute for Mathematics and Computing Advisory Board
- 2004–current ACM Onward Steering Committee Member

- 2014–2019 ACM/Usenix Symposium on Usable Privacy and Security Steering Committee Member
- 2009–2015 Hillside Patterns Group Board of Directors Member

Past seven years: editorial positions

- 2012–2018 IGI Global International Journal of Game-Based Learning Editorial Committee
- 2017 ACM SIGPLAN Onward Essays Chair
- 2012–current Elsevier Computers and Security Editorial Board Member
- 2015 ACM/Usenix Symposium on Usable Privacy and Security PC Chair
- 2015–current Springer Persuasive Technology Program Committee

6. GRADUATE SUPERVISIONS:

Current:

- PostDoctoral: 0.
- Doctoral: 3. (Alam, Zhou, Betts)
- Masters: 1. (Huayhua)

Career:

- PostDoctoral: 9.
- Masters: 44 completed.
- Doctoral: 16 completed.

Past seven years:

- Sami Huayhua, MHCI 2021-
- Lucas Betts, Ph.D. 2022- (Auckland)
- Sijie Zhou, Ph.D. 2020- (Auckland)
- Eric Spero, Ph.D. 2018-2023
- Son Vu Dang, M.Des. 2020-2023
- Aniqa Alam, Ph.D. 2021-current
- Lin Kyi, M.A. 2019-2021
- Vincere Ip, M.Des. 2017-2021
- Joshua Carr, M.A.Sc., H.C.I 2018-2020
- Alezandra Mesley, M.A. H.C.I 2018-2019
- Zahra Hassanzadeh, M.C.S, 2018-2019
- Eric Spero, M.A. HCI, 2016-2018
- Sumbal Maqsood, M.A. HCI, 2015-2018
- Peter Simonyi, M.C.S. 2015-2018
- Gerardo Escandon, M.A.Sc. HCI, 2014-2017
- Abdulrahmen Almouldi, M.C.S. HCI, 2014-2017
- Reza GhasemAghaei, Ph.D. Computer Science, 2012-2017
- Wahida Chowdhury, Ph.D. Cognitive Science, 2013-2017
- Milica Stojmenovic, Ph.D. Computer Science, 2015-2016 (Melbourne)
- Jeff Wilson, M.C.S. Computer Science, 2013–2015
- Peter Simonyi, M.C.S. Computer Science, 2013–2015
- Ravina Samaroo, M.A. Human-Computer Interaction, 2013–2015

- Elizabeth Stobert, Ph.D. Computer Science, 2011-2015

7. COURSES TAUGHT:

   Past seven years:

   - 2022: Carleton, HCIN5200, Software and User Interface Development
   - 2021: Carleton, HCIN5200, Software and User Interface Development
   - 2021: Carleton, COMP3008, Human-Computer Interaction
   - 2020: Carleton, HCIN5200, Software and User Interface Development
   - 2020: Carleton, COMP3008, Human-Computer Interaction
   - 2019: Carleton, HCIN5200, Software and User Interface Development
   - 2018: Carleton, COMP5209, Visual Analytics
   - 2018: Carleton, HCIN5200, Software and User Interface Development
   - 2018: Carleton, COMP3008, Human-Computer Interaction
   - 2017: Carleton, COMP3008, Human-Computer Interaction
   - 2017: Carleton, HCIN5200, Software and User Interface Development
   - 2015: Carleton, COMP3008, Human-Computer Interaction
   - 2015: Carleton, COMP5209, Visual Analytics
   - 2015: Carleton, COMP5209, Visual Analytics

8. EXTERNAL RESEARCH FUNDING:

   Note: All amounts reflect money directly available in CAD, and does not include overhead.

   Past seven years:

   - 2022: NSERC Discovery Grant, $145K, Secure Software Design and Development, 2022 was year 1 of 5
   - 2022: ISED National Consortium for Cybersecurity, $80M, 2022 was year 1 of 4
   - 2020: NSERC Post-Doctoral Fellowship, $45K (for Hala Assa, Declined for Tenure Track Appointment)
   - 2018: NSERC Post-Doctoral Fellowship, $45K (for Milica Stojmenovic)
   - 2017: MITACs Post-Doctoral Fellowship, $55K (for Milica Stojmenovic)
   - 2016: MITACs Post-Doctoral Fellowship, $55K (for Milica Stojmenovic)
   - 2016: NSERC Discovery Grant, $120K, New Directions in Usable (6 Years)
   - 2015: Dell Research Award, $24K, Mobile Authentication
   - 2015: NSERC CREATE Grant, $1.65M, Collaborative Learning of Usability Experiences (6 Years)
   - 2015: MITACs Post-Doctoral Internship, $45K (for Judith Brown)
   - 2014: Communications Security Establishment, $61K, Surface Computing Technology III
   - 2014: MITACs Post-Doctoral Fellowship, $50K (for Judith Brown)
   - 2013: Communications Security Establishment, $53K, Surface Computing Technology II
   - 2013: MITACs Post-Doctoral Fellowship, $50K (for Judith Brown)
   - 2012: Communications Security Establishment, $25K, Surface Computing Technology

   Earlier Major Funding:

   - 2010-2014: Industry Canada Network of Centres of Excellence (GRAND): 1 of 50, $25M
   - 2010-2014: NSERC Strategic Research Network (SurfNet): 1 of 14 co-PIs, $5M

- 2009-2013: NSERC Strategic Research Network (ISSNet): 1 of 14 co-PIs, $5M

9. PUBLICATIONS:

   Lifetime Summary:

   - Authored Books: 2
   - Edited Books: 5
   - Patents: 1
   - Refereed Book Chapters: 12
   - Refereed Journal Articles: 38
   - Refereed Conference Papers: 239
   - Non-Refereed Articles: 8

# Publications (Last 7 Years)

# References


[1] Sijie Zhuo, Robert Biddle, Lucas Betts, Nalin Asanka Gamagedara Arachchilage, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. What you see is not what you get: The role of email presentation in phishing susceptibility. *arXiv preprint arXiv:2304.00664*, 2023.

[2] Marc Sallin, Martin Kropp, Craig Anslow, and Robert Biddle. Waste self-reporting for software development productivity improvement. In *Agile Processes in Software Engineering and Extreme Programming: 24rd International Conference on Agile Software Development, XP 2023, Amsterdam, Netherlands, June 13–16, 2023, Proceedings*. Springer International Publishing Cham, 2023.

[3] Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. Sok: Human-centered phishing susceptibility. *ACM Transactions on Privacy and Security*, 2022.

[4] Aniqa Alam, Robert Biddle, and Elizabeth Stobert. This is different from the western world: Understanding password-sharing in bangladesh. In *Usable Security (USEC) 2023*. Internet Society, 2023.

[5] Milica Stojmenović, Eric Spero, Miloš Stojmenović, and Robert Biddle. What is beautiful is secure. *ACM Transactions on Privacy and Security*, 25(4):1–30, 2022.

[6] Johann Weichbrodt, Martin Kropp, Robert Biddle, Peggy Gregory, Craig Anslow, Ursina Maria Bühler, Magdalena Mateescu, and Andreas Meier. Understanding leadership in agile software development teams: Who and how? In *Agile Processes in Software Engineering and Extreme Programming: 23rd International Conference on Agile Software Development, XP 2022, Copenhagen, Denmark, June 13–17, 2022, Proceedings*, pages 99–113. Springer International Publishing Cham, 2022.

[7] Zahra Hassanzadeh, Sky Marsen, and Robert Biddle. User perception of data breaches. *IEEE Transactions on Professional Communication*, 2021.

[8] Robert Biddle, Martin Kropp, Andreas Meier, and Craig Anslow. Agile software development: Practices, self-organization, and satisfaction. In Manual Nicklich, Sabine Pfeiffer, and Stefan Sauer, editors, *The Agile Imperative. Teams, organizations and society under reconstruction?* Palgrave Macmillan, 2021.

[9] Robert Biddle and James Noble. Semiotics of the language of programs. In Amir Biglari, editor, *Open Semiotics*. L'Harmattan, 2021.

[10] Lavanya Sajwan, James Noble, Craig Anslow, and Robert Biddle. Why do programmers do what they do? A theory of influences on security practices. In *Proceedings of the Workshop on Usable Security and Privacy*. IEEE, 2021.

[11] Eric Spero and Robert Biddle. Out of sight, out of mind: UI design and the inhibition of mental models of security. In *Proceedings of the New Security Paradigms Workshop 2020*. Association for Computing Machinery, 2020.

[12] Eric Spero and Robert Biddle. Home and away: UI design patterns for supporting end-user security. In *Proceedings of the European Conference on Pattern Languages of Programs 2020*, EuroPLoP '20, New York, NY, USA, 2020. Association for Computing Machinery.

[13] Zahra Hassanzadeh, Sky Marsen, and Robert Biddle. We're here to help: Company image repair and user perception of data breaches. In *Proceedings of Graphics Interface 2020*. IEEE, 2020.

[14] Martin Kropp, Andreas Meier, Craig Anslow, and Robert Biddle. Satisfaction and its correlates in agile software development. *Journal of Systems and Software*, 164:110544, 2020.

[15] Eric Spero and Robert Biddle. Security begins at home: Everyday security behaviour and lessons for cybersecurity research. In *Proceedings of the Conference on Pattern Languages of Programs 2019*. Association for Computing Machinery, 2019.

[16] Steven L Greenspan, Robert Biddle, and Judith M Brown. Positioning a cursor on a display monitor based on a user's eye-gaze position, US Patent number 10372202, 2019.

[17] Eric Spero and Robert Biddle. Security begins at home: Everyday security behaviour and lessons for cybersecurity research. In *Proceedings of Pattern Languages of Programming*. ACM, 2019.

[18] M. Stojmenovic, E. Spero, T. Oyelowo, and R. Biddle. Website identity notification: Testing the simplest thing that could possibly work. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–7, Aug 2019.

[19] E. Spero, M. Stojmenović, Z. Hassanzadeh, S. Chiasson, and R. Biddle. Mixed pictures: Mental models of malware. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–3, Aug 2019.

[20] R. Biddle, J. M. Brown, and S. Greenspan. From incident to insight: Incident responders and software innovation. *IEEE Software*, 36(1):56–62, Jan 2019.

[21] Eric Spero, Milica Stojmenovic, Ali Arya, and Robert Biddle. Learning with trees: A non-linear e-textbook format for deep learning. In *Proceedings of HCI International*, Orlando, USA, 2019.

[22] M. Stojmenovic and R. Biddle. Hide-and-seek with website identity information. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–6, Aug 2018.

[23] Elizabeth Stobert and Robert Biddle. The password life cycle. *ACM Transactions on Privacy and Security (TOPS)*, 21(3):13, 2018.

[24] Muye Jiang, Gerry Chan, and Robert Biddle. Sports analytics: Visualizing basketball records in graphical form. In *Data Analytics: Concepts, Techniques and Applications*. CRC Press, Taylor & Francis Group, 2018.

[25] Martin Kropp Robert Biddle, Andreas Meier and Craig Anslow. Myagile: Sociological and cultural effects of agile on teams and their members. In *IEEE/ACM 11th International Workshop on Cooperative and Human Aspects of Software*. ACM, 2018.

[26] Martin Kropp Robert Biddle, Andreas Meier and Craig Anslow. Satisfaction, practices, and influences in agile software development. In *Evaluation and Assessment in Software Engineering*. ACM, 2018.

[27] Martin Kropp, Andreas Meier, and Robert Biddle. Stress in agile software development:

Practices and outcomes. In *19th International Conference on Agile Software Development*. IEEE, 2018.

[28] Milica Stojmenovic, Robert Biddle, John Grundy, and Vivienne Farrell. The influence of textual and verbal word-of-mouth on website usability and visual appeal. *The Journal of Supercomputing*, pages 1–48, 2018.

[29] Milica Stojmenović, Temitayo Oyelowo, Alisa Tkaczyk, and Robert Biddle. Building website certificate mental models. In *International Conference on Persuasive Technology*, pages 242–254. Springer, 2018.

[30] Reza GhasemAghaei, Ali Arya, and Robert Biddle. Affective walkthroughs and heuristics: Evaluating minecraft hour of code. In *International Conference on Learning and Collaboration Technologies*. Springer International Publishing, 2017.

[31] Milica Stojmenovic, John Grundy, Vivienne Farrel, Leonard Hoon, and Robert Biddle. Does textual word-of-mouth affect look and feel? perceived and objective usability and visual appeal in a website domain with a less developed mental model. In *Proceedings of the 28th Australian computer-human interaction conference on designing futures: the future of design*, pages 316–323. ACM, 2016.

[32] Elizabeth Stobert, Carrie Gates, Irwin Reyes, and Robert Biddle. Mobile device security: Hopes and fears. In *International Conference on Passwords*, pages 3–20. Springer International Publishing, 2016.

[33] Martin Kropp, Judith M. Brown, Craig Anslow, Stevenson Gossage, Magdalena Mateescu, and Robert Biddle. Interactive digital cardwalls for agile software development. In *Collaboration Meets Interactive Spaces*, pages 287–318. Springer International Publishing, 2016.

[34] Judith M. Brown, Jeff Wilson, Peter Simonyi, Miran Mirza, and Robert Biddle. Surface applications for security analysis. In *Collaboration Meets Interactive Spaces*, pages 391–423. Springer International Publishing, 2016.

[35] Martin Kropp, Andreas Meier, and Robert Biddle. Agile practices, collaboration and experience: An empirical study about the effect of experience in agile software development. In *Product-Focused Software Process Improvement: 17th International Conference, PROFES 2016, Trondheim, Norway, November 22-24, 2016, Proceedings 17*, pages 416–431. Springer International Publishing, 2016.

[36] Hala Assal, Sonia Chiasson, and Robert Biddle. Cesar: Visual representation of source code vulnerabilities. In *Visualization for Cyber Security (VizSec), 2016 IEEE Symposium on*, pages 1–8. IEEE, 2016.

[37] Craig Anslow, Stuart Marshall, James Noble, and Robert Biddle. Hacking with multi-touch for java (mt4j). In *Proceedings of the 1st International Workshop on Mobile Development*, pages 17–20. ACM, 2016.

[38] Reza GhasemAghaei, Ali Arya, and Robert Biddle. A dashboard for affective e-learning: Data visualization for monitoring online learner emotions. In *EdMedia: World Conference on Educational Media and Technology*, volume 2016, pages 1536–1543, 2016.

[39] Reza GhasemAghaei, Ali Arya, and Robert Biddle. Evaluating software for affective education: A case study of affective heuristics. In *EdMedia: World Conference on Educational Media and Technology*, volume 2016, pages 573–580, 2016.

[40] Reza GhasemAghaei, Ali Arya, and Robert Biddle. Evaluating software for affective education: A case study of the affective walkthrough. In *International Conference on Human-Computer Interaction*, pages 226–231. Springer International Publishing, 2016.

[41] Reza GhasemAghaei, Ali Arya, and Robert Biddle. Made ratio: Affective multimodal software for mathematical concepts. In *International Conference on Learning and Collaboration*

*Technologies*, pages 487–498. Springer International Publishing, 2016.

[42] Leah Zhang-Kennedy, Elias Fares, Sonia Chiasson, and Robert Biddle. Geo-phisher: the design and evaluation of information visualizations about internet phishing trends. In *Electronic Crime Research (eCrime), 2016 APWG Symposium on*, pages 1–12. IEEE, 2016.

[43] Judith M. Brown, Steven Greenspan, and Robert Biddle. Incident response teams in it operations centers: the T-TOCs model of team functionality. *Cognition, Technology & Work*, pages 1–22, 2016.

[44] Martin Kropp, Andreas Meier, and Robert Biddle. Teaching agile collaboration skills in the classroom. In *2016 IEEE 29th International Conference on Software Engineering Education and Training (CSEET)*, pages 118–127. IEEE, 2016.

[45] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, 32(3):215–257, 2016.

[46] B. Freitas, A. Matrawy, and R. Biddle. Online neighborhood watch: The impact of social network advice on software security decisions. *Canadian Journal of Electrical and Computer Engineering*, 39(4):322–332, Fall 2016.

[47] Leah Zhang-Kennedy, Elias Fares, Sonia Chiasson, and Robert Biddle. The effects of interactivity on information visualization about internet phishing trends. In *APWG eCrime*. IEEE, 2016.

[48] Elizabeth Stobert and Robert Biddle. Expert password management. *Proc. Passwords*, 2015.

[49] Reza GhasemAghaei, Ali Arya, and Robert Biddle. Made ratio: Affective multimodal software for mathematical concepts. In *HCI International*, Toronto, Canada, 2015. Springer.

[50] Peter Simonyi, Jeff Wilson, Judith M. Brown, and Robert Biddle. Supporting "what-if" in touch-screen web applications. In *Workshop on Programming for Mobile and Touch*, Pittsburgh, USA, September 2015. ACM.

[51] Miran Mirza, Jeff Wilson, and Robert Biddle. Collaborative annotations for large touchscreen web applications. In *Workshop on Programming for Mobile and Touch*, Pittsburgh, USA, September 2015. ACM.

[52] Alain Forget, Sonia Chiasson, and Robert Biddle. Choose your own authentication. In *New Security Paradigm Workshop (NSPW)*. ACM, 2015.

[53] Alain Forget, Sonia Chiasson, and Robert Biddle. User-centred authentication feature framework. *Journal of Information Management and Computer Security*, 23, 2015.

[54] Reza GhasemAghaei, Ali Arya, and Robert Biddle. Design practices for multimodal affective mathematical learning. In *International Symposium on Computer Science and Software Engineering*, Tabriz, Iran, August 2015. IEEE.

[55] Robert Biddle Stevenson Gossage, Judith M. Brown. Understanding digital cardwall usage. In *Proceedings of the Agile Software Development Conference*, Washington D.C., 2015. IEEE.

[56] Reza GhasemAghaei, Ali Arya, and Robert Biddle. Multimodal software for affective education: Ui evaluation. In *Ed-Media: World Conference on Educational Multimedia, Hypermedia, and Telecommunications*, Montreal, Canada, 2015. Association for the Advancement of Computing in Education.

[57] Reza GhasemAghaei, Ali Arya, and Robert Biddle. Multimodal software for affective education: Ui design. In *Ed-Media: World Conference on Educational Multimedia, Hypermedia, and Telecommunications*, Montreal, Canada, 2015. Association for the Advancement of Computing in Education.

[58] Reza GhasemAghaei, Ali Arya, and Robert Biddle. The made framework: Multimodal software for affective education. In *Ed-Media: World Conference on Educational Multimedia,*

*Hypermedia, and Telecommunications*, Montreal, Canada, 2015. Association for the Advancement of Computing in Education.

**Dr. Sonia Chiasson**

Professor, Co-Director of HCI Graduate Program
NSERC Arthur B. McDonald Fellow
School of Computer Science, Carleton University, Ottawa Canada
chiasson@scs.carleton.ca http://chorus.scs.carleton.ca (613) 520-2600x1656

**Funding Summary**

$250,000 for NSERC Arthur. B. McDonald Fellowship
$1,781,887 for Research, Infrastructure and Equipment
from NSERC, ERA, OPC, CIRA, MITACS, eCampus Ontario, NIST, Bluink
including *Early Researcher Award and NSERC Discovery Accelerator supplement*

$1,000,000 for Canada Research Chair (renewed, 2 terms)

$2,800,000 for NCE-Knowledge Mobilization (co-investigator) (renewed, 2 terms)

$1,650,000 for NSERC CREATE (co-investigator)

$2,500,000 for SSHRC Partnership Grant (co-investigator)

**Publications Summary**

6327 citations, h-index: 35

17 journal articles

65 fully refereed conference papers

**Supervision Summary**

*2017 Faculty Graduate Mentoring Award*

1 Postdoc, 6 PhD, 24 Masters completed

2 PhD, 2 Masters in-progress

36 Undergraduates (honours thesis/project, coop, research assistants)

**Leadership Highlights**

Deputy Scientific Director, SERENE-RISC NCE-KM

55 invited talks, panels, guest lectures

USENIX SOUPS Technical Program Co-Chair for 2017 and 2018, General Chair 2021 and 2022.

**Teaching Summary**

*2014 Excellence Award in Graduate Teaching*

Carleton University Teaching: HCIN5100, HCIN5200 (Software and User Interface Development), COMP5110 (Computer Security and Usability), COMP 3008 (Human Computer Interaction)

University of Saskatchewan: full-time undergraduate instructor 2001 – 2005

## 1. Funding

### Awarded

| | | |
|---|---|---|
| 2023 – 2029<br>Principal Investigator | Improving Usable Privacy and Security through Universal Design<br>NSERC Discovery Grant<br>$52,000/year for 5 years | $260,000 |
| 2022<br>Principal Investigator | Research Excellence Award<br>Carleton University Faculty of Science | $5,000 |
| 2023 – 2025<br>Principal Investigator | Arthur B. McDonald Fellowship<br>NSERC award<br>$125,000/year for 2 years | $250,000 |
| 2022<br>Principal Investigator | Summer funding for students<br>Carleton Coop Employer (CCE) funding ($4000)<br>DSRI ($5000 * 2 students)<br>USRA ($6000) | $20,000 |
| 2021 – 2025<br>Co-investigator | Cyber Security Innovation Network (CSIN),<br>National Cybersecurity Consortium (NCC – led by University of Calgary, Concordia University, University of New Brunswick, Ryerson University and University of Waterloo)<br>Innovation, Science and Economic Development Canada<br>Co-investigator in the Human-Centric Cybersecurity group<br>$20M/year for 4 years across entire network | $80,000,000 |
| 2021<br>Principal Investigator | Summer funding for students<br>*Carleton Coop Employer (CCE) funding ($4000)*<br>*DSRI ($5000)*<br>*USRA ($6000)* | $15,000 |
| 2021 – 2026<br>Co-investigator | Human-Centric Cybersecurity (H2C) Partnership<br>SSHRC Partnership Grant. Benoit Dupont (PI) + 33 others, Sonia Chiasson is Leader of the Behavioural Research Cluster and EDI Champion<br>$500,000/year for 5 years<br><br>2022 Mental models of privacy mini-grant: $5,000<br>2023 Security & Privacy in Healthcare for older adults mini-grant: $25,000 | $2,500,000 |
| 2021<br>Principal Investigator | Understanding and increasing diversity in Computer Science<br>Carleton Research Achievement Award | $15,000 |
| 2020<br>Principal Investigator | Summer funding for students<br>Carleton Coop Employer (CCE) funding ($4000 * 2 students)<br>ITAC Career Ready program ($7000 + $5000)<br>I-CUREUS Summer Program ($8400) | $28,400 |
| 2018 – 2021 | SERENE - Smart Cybersecurity Network (Renewal) | $1,200,000 |

| | | |
|---|---|---|
| Deputy Scientific Director | NSERC/SSHRC Networks of Centres of Excellence for Knowledge Mobilization (NCE-KM). Benoit Dupont (PI and Scientific Director, U de Montreal), Sonia Chiasson (Deputy Scientific Director)<br>$400,000/year for 3 years | |
| 2017 – 2018<br>Principal Investigator | Accessible and Usable Security: An evaluation of screen-reader users' online security and privacy strategies<br>eCampus Ontario Digital Inclusion Research<br>Co-lead: Daniela Napoli, Masters student | $20,000 |
| 2017 – 18 | Bluink – industry donation in support of the CHORUS Lab | $20,000 |
| 2017 – 20<br>Principal Investigator | Human oriented computer security<br>NSERC Discovery Accelerator Supplement<br>$40,000/year for 3 years | $120,000 |
| 2017 – 22<br>Principal Investigator | Human oriented computer security<br>NSERC Discovery Grant<br>$34,000/year for 5 years | $170,000 |
| 2017 – 22<br>Principal Investigator | Tier 2 Canada Research Chair (Renewal)<br>in User-Centric Cybersecurity<br>$100,000/year for 5 years towards salary | $500,000 |
| 2016<br>Principal Investigator | Child Login Research using FIDO public key authentication<br>NSERC Engage Grant with Bluink | $25,000 |
| 2016 – 21<br>Principal Investigator | Usable Privacy and Security for Children<br>Early Research Award (ERA)<br>Ontario Research Fund<br>$30,000/yr for 5 years | $150,000 |
| 2015 – 18<br>Principal Investigator | Designing children's cybersecurity games for real-world behaviour change<br>Student: Sana Maqsood, PhD, Sept 2015 – Aug 2018<br>MITACS PhD Fellowship in partnership with MediaSmarts<br>$30,000/yr for 3 years | $90,000 |
| 2015<br>Principal Investigator | Exploring the use of the Media Equation in children's educational cybersecurity game<br>Student: Christine Mekhail, Masters of HCI<br>MITACS Accelerate grant in partnership with MediaSmarts | $15,000 |
| 2015 – 16<br>Principal Investigator | User authentication for children<br>CIRA Community Investment Program | $42,500 |
| 2015 – 16<br>Principal Investigator | Improving security and privacy behaviour and awareness for children<br>Office of the Privacy Commissioner of Canada Contributions Program | $50,000 |
| 2015 – 21<br>Co-investigator | Collaborative Learning of Usability Experiences (CLUE)<br>NSERC Collaborative Research and Training Experience Program (CREATE).<br>Anthony Whitehead (Principal Investigator) + 8 others | $1,650,000 |

| | | |
|---|---|---|
| | $275,000/year for 6 years | |
| 2014 – 18<br>Deputy Scientific Director | SERENE - Smart Cybersecurity Network<br>NSERC/SSHRC Networks of Centres of Excellence for Knowledge Mobilization (NCE-KM). Benoit Dupont (PI and Scientific Director, U de Montreal), Sonia Chiasson (Deputy Scientific Director)<br>$400,000/year for 4 years | $1,600,000 |
| 2013 – 14<br>Principal Investigator | Carleton's Human Oriented Research in Usable Security (CHORUS) Lab<br>Leaders Opportunity Fund, Canada Foundation for Innovation (CFI)<br>Ontario Research Fund (ORF) | $250,000 |
| 2013 – 14<br>Principal Investigator | Adapting CAPTCHAs for smart phone usage<br>Special Project award from the NSERC Surfnet Strategic Network<br>with Gerardo Reynaga (PhD student) and Robert Biddle | $25,000 |
| 2013 – 14<br>Principal Investigator | Improving mental models of security and privacy through visualizations<br>Office of the Privacy Commissioner of Canada Contributions Program | $50,000 |
| 2012 – 15<br>Collab. Network Investigator | Privacy and Security in New Media project<br>NSERC/SSHRC GRAND – Graphics, Animation, and New Media Networks of Centres of Excellence (NCE)<br>2012 -- $9,000; 2013 -- $15,000; 2014 -- $8,000 | $32,000 |
| 2012 – 17<br>Principal Investigator | Universal Usable Security<br>NSERC Discovery Grant<br>$22,000/year for 5 years | $110,000 |
| 2012 – 17 | Institutional Canada Research Chair support<br>Carleton University<br>$10,000/year for 5 years | $50,000 |
| 2012 – 17<br>Principal Investigator | Tier 2 Canada Research Chair<br>in Human Oriented Computer Security<br>$100,000/year for 5 years towards salary | $500,000 |
| 2011 – 13<br>Co-PI | Human Behaviour and Computer Security<br>NSERC ISSNet Strategic Network<br>2011 - $20,000<br>2012 - $57,487<br>2013 - $11,500 | $88,987 |
| 2010 – 12<br>Principal Investigator | Understanding and Influencing End-User Comprehension of Computer Security Threats and Defenses,<br>US National Institute of Standards and Technology, NIST 2010-MSE-01,<br>with Robert Biddle (Co-PI)<br>$50,000/year for 2 years | $100,000 |
| 2011 | Institutional start-up funding<br>Carleton University | $65,000 |

## 2. Employment History

| | |
|---|---|
| 2023 – 25 | NSERC McDonald Fellow<br>School of Computer Science, Carleton University |
| 2022 – | Full Professor<br>Co-Director, HCI Graduate Program<br>School of Computer Science, Carleton University |
| 2017 – 21 | Canada Research Chair in User-Centric Cybersecurity, Tier 2 (renewal)<br>School of Computer Science, Carleton University |
| 2016 – 22 | Associate Professor (as of July 1 2016)<br>School of Computer Science, Carleton University |
| 2012 – 17 | Canada Research Chair in Human Oriented Computer Security, Tier 2<br>School of Computer Science, Carleton University |
| 2011 - 16 | Assistant Professor (tenured as of July 1, 2015)<br>School of Computer Science, Carleton University |
| 2009 – 11 | Post Doctoral Fellow, School of Computer Science<br>NSERC ISSNet strategic network, Carleton University |
| 2005 – 08 | Research Assistant, Teaching Assistant<br>School of Computer Science, Carleton University |
| 2001 – 05 | Instructor and Coordinator for Introduction to CS course (full-time)<br>Department of Computer Science, University of Saskatchewan |
| 2000 | Sessional Instructor, Introduction to CS<br>Department of Computer Science, University of Saskatchewan |
| 1999 – 01 | Teaching assistant<br>Department of Computer Science, University of Saskatchewan |
| 1999 | Contract – Curriculum development<br>New Brunswick Department of Education, Fredericton, NB |
| 1997 | Junior Network Analyst<br>Maritime Information Technology, Fredericton, NB |

## 3. Publications

| | All | Since 2018 |
|---|---|---|
| Citations* | 6480 | 2985 |
| h-index* | 36 | 29 |
| i10-index* | 77 | 64 |

(*according to Google Scholar, August 2023. Google Scholar is used because neither SCOPUS nor Web of Science offer adequate coverage of Security and HCI publications)

### Manuscripts in submission

[M1] **S.G. Morkonda,** S. Chiasson, P.C. van Oorschot. Influences of Displaying Permission-related Information On Web Single Sign-On Login Decisions, (Submitted to Elsevier's Computers & Security, 2023)

[M2] **S.G. Morkonda,** S. Chiasson, P.C. van Oorschot. "Sign in with ... Privacy": Timely Disclosure of Privacy Differences among Web SSO Login Options (Submitted to ACM Transactions on Privacy and Security, 2023)

[M3] **K. Baig, D. Napoli,** S. Chiasson. A comparison of users' and non-users' perceptions of health and ancestry at-home DNA testing (Submitted to EuroUSEC 2023)

[M4] **K. Chaudhry, A.L Theus**, H. Assal, S. Chiasson. ``It's not that I want to see the student's bedroom...": Instructor Perceptions of e-Proctoring Software (Submitted to EuroUSEC 2023)

**Articles in refereed publications (journals)**

[J17] M. Hull, L. Zhang-Kennedy, **K. Baig**, S. Chiasson (2021). Understanding Individual Differences: Factors Affecting Secure Computer Behaviour. Behaviour & Information Technology (TBIT)

[J16] **J. Rocheleau,** S. Chiasson (2021). Privacy and Safety on Social Networking Sites: Autistic and Non-Autistic Teenagers' Attitudes and Behaviors. ACM Transactions on Computer Human Interaction (TOCHI) [*A*-ranked*]

[J15] **S. Maqsood**, S. Chiasson (2021). The design, development, and evaluation of a cybersecurity and privacy game for tweens. ACM Transactions on Privacy & Security (TOPS) *[A]*

[J14] L. Zhang-Kennedy, S. Chiasson (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. ACM Computing Surveys (CSUR), 54(1), p. 1–39. *[A*]*

[J13] **H. Assal, A. Imran**, S. Chiasson (2018). An Exploration of Graphical Password Authentication for Children. International Journal of Child-Computer Interaction, November, Elsevier.

[J12] **F. Lalonde Levesque**, S. Chiasson, A. Somayaji, J.M. Fernandez (2018). Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial approach, Transactions on Privacy and Security (TOPS), July, ACM. *[A]*

[J11] **L. Zhang-Kennedy, Y. Abdelaziz**, S. Chiasson (2017). Cyberheroes: The Design and Evaluation of an Interactive Ebook to Educate Children about Online Privacy. International Journal of Child-Computer Interaction, Elsevier, July, 13(1), p. 10-18

[J10] **F. Chanchary, Y. Abdelaziz**, S. Chiasson (2018). Sharing, Advertising, and Tracking in an Online World. IEEE Internet Computing 22(2), p. 52-61

[J9] **S. Maqsood**, S. Chiasson, A. Girouard (2016). Bend Passwords: Using Gestures to Authenticate on Flexible Devices. Personal and Ubiquitous Computing, Springer, 20(4), p573-600

[J8] **L. Zhang-Kennedy**, S. Chiasson, and R. Biddle (2016). The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cyber Security. International Journal of Human-Computer Interaction, Taylor & Francis, 32(3), p. 215-257

[J7] A. Forget, S. Chiasson, and R. Biddle (2015). User-centred authentication feature framework. Journal of Information Management and Computer Security, 23(5), p. 497 - 515

[J6] S. Chiasson and P. C. van Oorschot (2015). Quantifying the security advantage of password expiration policies. Designs, Codes and Cryptography (DESI), 77(2), p.401-408.

[J5] **M. Alsharnouby, F. Alaca**, and S. Chiasson (2015). Why phishing still works: User strategies for combating phishing attacks. Int. Journal of Human-Computer Studies (Elsevier), 82:69 – 82

[J4] **Y. Xu, G. Reynaga**, S. Chiasson, J.-M. Frahm, F. Monrose, P.C. van Oorschot (2014) Security Analysis and Related Usability of Motion-based CAPTCHAs: Decoding Codewords in Motion. IEEE Trans. on Dependable and Secure Computing, Sept/Oct, 11(5), p. 480 – 493. *[A]*

[J3] S. Chiasson, **E. Stobert, A. Forget**, R. Biddle (2012). Persuasive Cued Click-Points: Design and Evaluation. IEEE Trans. on Dependable & Secure Computing (TDSC), Mar/Apr, p. 222-235. *[A]*

[J2] R. Biddle, S. Chiasson, P.C. van Oorschot (2011). Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys 44(4), p. 19:1--19:41. (Authors in alphabetical order). *[A*]*

[J1] S. Chiasson, **A. Forget**, R. Biddle, P.C. van Oorschot (2009). User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security 8(5), p. 387-398.

**Other refereed contributions (fully refereed conference papers)**

[C66] **P. Chametka**, S. Maqsood, S. Chiasson (2023). Security and Privacy perceptions of mental health chatbots. Privacy, Security, and Trust (PST) (to appear)

[C65] **A.-L. Theus**, S. Chiasson (2023). "A solution to a problem that didn't exist?": Exploring Attitudes Towards Smart Streetlighting Systems". INTERACT (to appear)

[C64] **M. Keleher, P. Nagabandi**, S. Maqsood, S. Chiasson (2022). How well do experts understand end-users' perceptions of manipulative patterns? NordiCHI.

[C63] F. Westin, K. Hundlani, S. Chiasson (2022). "I just want to play games with friends and it asked me for all of my information": Trading privacy for connection during the COVID-19 pandemic. EuroUSEC.

[C62] **S.G. Morkonda,** S. Chiasson, P.C. van Oorschot (2021). Empirical Analysis and Privacy Implications in OAuth-based Single Sign-On Systems. WPES (20% accept rate).

[C61] **K. Baig,** K. Hundlani, E. Kazan, S. Chiasson (2021)**.** Replication: Effects of Media on the Mental Models of Technical Users. Symposium on Usable Privacy and Security (SOUPS), USENIX (26% accept rate).

[C60] **D. Napoli, K. Baig, S. Maqsood**, S. Chiasson (2021). "I'm Literally Just Hoping This Will Work": Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities. Symposium on Usable Privacy and Security (SOUPS), USENIX (26% accept rate).

[C59] L. Zhang-Kennedy, S. Chiasson (2021). "Whether it's moral is a whole other story": Consumer perspectives on privacy regulations and corporate data practices. Symposium on Usable Privacy and Security (SOUPS), USENIX (26% accept rate).

[C58] **E. Ulqinaku**, H. Assal, A. Abdou, S. Chiasson, S. Čapkun (2021). Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols. USENIX Security 2021 (18.8% accept rate*). [A*]*

[C57] **F. Westin,** S. Chiasson (2021). "It's So Difficult to Sever that Connection": The Role of FoMO in Users' Reluctant Privacy Behaviours. ACM CHI 2021 (26% accept rate**,** ***Honorable Mention Award:Top 5%).*** *[A*]*

[C56] **S. Maqsood,** S. Chiasson (2021). "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. ACM CHI 2021 (26% accept rate). *[A*]*

[C55] **M. Lutaaya,** H. Assal**, K. Baig, S. Maqsood,** S. Chiasson (2021)**.** "Lose Your Phone, Lose Your Identity": Exploring Users' Perceptions and Expectations of a Digital Identity Service. USEC, Internet Society.

[C54] **K. Baig, R. Mohamed, A.-L. Theus,** S. Chiasson (2020). "I'm hoping they're an ethical company that won't do anything that I'll regret": Users Perceptions of At-home DNA Testing Companies. ACM CHI 2020 (24% accept rate). *[A*]*

[C53] **R. Jeong,** S. Chiasson (2020). `Lime', `Open Lock', and `Blocked': Children's Perception of Colors, Symbols, and Words in Cybersecurity Warnings. ACM CHI 2020 (24% accept rate). *[A*]*

[C52] **S. Gabriele**, S. Chiasson (2020). Step it up! What is your fitness tracker sharing? ACM CHI 2020 (24% accept rate). *[A*]*

[C51] **R. Mohamed**, S. Chiasson (2020). Hire Me, I Have an Awesome Facebook Profile: The Influence of Aging Visualizations on Hiring Decisions. ACM CHI 2020 (24% accept rate). *[A*]*

[C50] **F. Westin**, S. Chiasson (2019). Opt Out of Privacy or "Go Home": Understanding Reluctant Privacy Behaviours through the FoMO-Centric Design Paradigm. New Security Paradigms Workshop (NSPW) 2019.

[C49] **E. Spero, M. Stojmenovic**, S. Chiasson, R. Biddle (2019). Control and Understanding in Malware and Software. APWG eCrime 2019.

[C48] **Y. Abdelaziz, D. Napoli**, S. Chiasson (2019). End-users and service providers: trust and distributed responsibility for account security. Submitted to Privacy, Security, and Trust (PST) 2019.

[C47] H. Assal, S. Chiasson (2019). "Think secure from the beginning": A survey with software developers. ACM CHI 2019 (23% accept rate, ***Best Paper Award: Top 1%***). *[A*]*

[C46] L. Zhang-Kennedy, **H. Assal, J. Rocheleau, R. Mohamed, K. Baig**, S. Chiasson (2018). The aftermath of a crypto-ransomware attack at a large academic institution, USENIX Security (19% accept rate). *[A*]*

[C45] **R. Mohamed**, S. Chiasson (2018). Online Privacy and Aging of Digital Artifacts. Symposium on Usable Privacy and Security (SOUPS), USENIX (23% accept rate).

[C44] **H. Assal**, S. Chiasson (2018). Security in the Software Development Lifecycle. Symposium on Usable Privacy and Security (SOUPS), USENIX (23% accept rate).

[C43] **S. Maqsood, C. Mekhail**, S. Chiasson (2018). A Day in the Life of Jos: A Web-based Game to Increase Children's Digital Literacy. Interaction Design and Children (IDC), ACM.

[C42] **R. Cooper, H. Assal,** S. Chiasson (2017). Cross-national privacy concerns on data collection by government agencies. IEEE Privacy, Security, and Trust.

[C41] **L. Zhang-Kennedy, K. Baig**, S. Chiasson (2017). Comics as Persuasion for Children's Online Privacy Education. British HCI.

[C40] **K. Hundlani**, S. Chiasson, L. Hamid (2017). No passwords needed: The iterative design of a parent-child authentication mechanism. MobileHCI, ACM (20% accept rate)

[C39] **R. Mohamed, T. Bardini Idalino**, S. Chiasson (2017). When private and professional lives meet: The impact of digital footprints on employees and political candidates. Social Media & Society, ACM

[C38] **B. Obada-Obieh**, S. Chiasson, A. Somayaji (2017). "Don't Break My Heart!": User Security Strategies for Online Dating. USEC, Internet Society (19% accept rate)

[C37] **H. Assal**, S. Chiasson, R. Biddle (2016). Cesar: Visual representation of source code vulnerabilities. VizSec, IEEE

[C36] **S. Hurtado**, S. Chiasson (2016). An Eye-tracking Evaluation of Driver Distraction and Unfamiliar Road Signs. Automotive 'UI, ACM

[C35] **L. Zhang-Kennedy**, **C. Mekhail, Y. Abdelaziz**, and S. Chiasson (2016). From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In Interaction Design and Children (IDC). ACM.

[C34] **L. Zhang-Kennedy**, **E. Fares,** S. Chiasson, and R. Biddle (2016). The effects of interactivity on information visualization about internet phishing trends. In APWG eCrime. IEEE.

[C33] **L. Zhang-Kennedy**, S. Chiasson, and P. C. van Oorschot (2016). Revisiting password rules: Facilitating human management of passwords. In APWG eCrime. IEEE.

[C32] **M. Baslyman** and S. Chiasson (2016). Smells phishy? An educational game about online phishing scams. In APWG eCrime. IEEE.

[C31] **G. Reynaga**, S. Chiasson, and P. C. van Oorschot (2015). Heuristics for the evaluation of captchas on smartphones. In British HCI Conference. ACM.

[C30] **G. Reynaga**, S. Chiasson, and P. C. van Oorschot (2015). Exploring the usability of captchas on smartphones: Comparisons and recommendations. In NDSS Workshop on Usable Security (USEC). Internet Society.

[C29] A. Forget, S. Chiasson, and R. Biddle (2015). Choose Your Own Authentication. In New Security Paradigm Workshop (NSPW). ACM. (accept rate 36%)

[C28] **F. Chanchary** and S. Chiasson (2015). User perceptions of sharing, advertising, and tracking. In Symposium on Usable Privacy and Security (SOUPS). USENIX. (accept rate 24%)

[C27] **H. Assal, S. Hurtado, A. Imran**, and S. Chiasson (2015). What's the deal with privacy apps? A comprehensive exploration of user perception and usability. In Mobile and Ubiquitous Multimedia (MUM). ACM.

[C26] **L. Zhang-Kennedy**, S. Chiasson, and R. Biddle (2014). Stop clicking on 'update later': Persuading users they need up-to-date antivirus protection. In International Conference on Persuasive Technology (PERSUASIVE), pages 302–322. Springer LNCS. (accept rate 31%)

[C25] **C. Grimm** and S. Chiasson (2014). Survey on the fate of digital footprints after death. In Workshop on Usable Security (USEC). Internet Society.

[C24] **L. Zhang-Kennedy**, S. Chiasson, and R. Biddle (2013). Password advice shouldn't be boring: Visualizing password guessing attacks. In APWG eCrime, pages 1–11. IEEE.

[C23] **G. Reynaga** and S. Chiasson (2013). The usability of captchas on smartphones. In Int. Conference on Security and Cryptography (SECRYPT), pages 427–434. SCITEPRESS.

[C22] **F. Lalonde Levesque, J. Nsiempba**, J. Fernandez, S. Chiasson, and A. Somayaji (2013). A clinical study of risk factors related to malware infections. In SIGSAC Conference on Computer and Communications Security (CCS), pages 97–108. ACM. (accept rate 20%) *[A*]*

[C21] **H.-Y. Chiang** and S. Chiasson (2013). Improving user authentication on mobile devices: A touch-screen graphical password. In Int. Conference on MobileHCI, pages 251–260. ACM. (accept rate 22%)

[C20] **V. Boothroyd** and S. Chiasson (2013). Writing down your password: Does it help? In Annual International Conference on Privacy, Security and Trust (PST), pages 267–274. IEEE.

[C19] **Y. Xu, G. Reynaga**, S. Chiasson, J.-M. Frahm, F. Monrose, and P. C. van Oorschot (2012). Security and usability challenges of moving-object captchas: Decoding codewords in motion. In USENIX Security Symposium. (accept rate 19%) *[A*]*

[C18] **D. McCarney, D. Barrera**, J. Clark, S. Chiasson, and P. C. van Oorschot (2012). Tapas: Design, implementation, and usability evaluation of a password manager. In Annual Computer Security Applications Conference (ACSAC), pages 89–98. ACM. (accept rate 19%)

[C17] **M. Mahmoud**, S. Chiasson, and A. Matrawy (2012). Does context influence responses to firewall warnings? In APWG eCrime, pages 1–10. IEEE.

[C16] **F. Lalonde Levesque,** C. Davis, J. Fernandez, S. Chiasson, and A. Somayaji (2012). Methodology for a field study of anti-malware software. In Workshop on Usable Security (USEC), Financial Cryptography and Data Security (FC), pages 80–85. Springer (LNCS).

[C15] **A. Forget**, S. Chiasson, and R. Biddle (2012). Supporting learning of an unfamiliar authentication scheme. In E-LEARN, pages 1002–1011. AACE.

[C14] S. Chiasson, **C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan,** and R. Biddle (2012). The MVP web-based authentication framework. In International Conference on Financial Cryptography and Data Security (FC), pages 16–24. Springer.

[C13] S. Chiasson, **M. Modi**, and R. Biddle (2011). AuctionHero: The design of a game to learn and teach about computer security. In E-LEARN. AACE.

[C12] **E. Stobert**, **A. Forget**, S. Chiasson, P.C. van Oorschot, R. Biddle (2010). Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords. Annual Computer Security Applications Conference (ACSAC). (17% accept rate).

[C11] **A. Forget**, S. Chiasson, R. Biddle (2010). Shoulder-Surfing Resistance with Eye-Gaze Entry in Click-Based Graphical Passwords (CHI Note). ACM SIGCHI Conference on Human Factors in Computing Systems (CHI). (22% accept rate).

[C10] S. Chiasson**, A. Forget, E. Stobert**, P.C. van Oorschot, R. Biddle, (2009). Multiple password interference in text and click-based graphical passwords. ACM Computer and Communications Security (CCS) (18% accept rate). *[A*]*

[C9] **S. Chiasson, A. Forget**, R. Biddle, P.C. van Oorschot (2008). Influencing Users Towards Better Passwords: Persuasive Cued Click-Points. British Computer Society HCI Conference (29% accept rate).

[C8] **A. Forget, S. Chiasson**, P.C. van Oorschot, R. Biddle (2008). Improving Text Passwords Through Persuasion. ACM Symposium on Usable Privacy and Security (SOUPS) (28% accept rate).

[C7] **A. Forget, S. Chiasson**, P.C. van Oorschot, R. Biddle (2008). Persuasion for Stronger Passwords: Motivation and Pilot Study. 3rd Conf. on Persuasive Technology, Springer LNCS.

[C6] **S. Chiasson**, J. Srinivasan, R. Biddle, P.C. van Oorschot (2008). Centered Discretization with Application to Graphical Passwords. USENIX Usability, Psychology, and Security (UPSEC).

[C5] **A. Forget, S. Chiasson**, R. Biddle (2007). Persuasion as Education for Computer Security. AACE World Conference on E-Learning in Corporate, Government, Healthcare & Higher Education (E-LEARN).

[C4] **S. Chiasson,** P.C. van Oorschot, R. Biddle (2007). Graphical Password Authentication Using Cued Click Points. European Symposium Research Computer Security (ESORICS), Springer LNCS. (24% accept rate).

[C3] **S. Chiasson**, R. Biddle, P.C. van Oorschot (2007). A Second Look at the Usability of Click-based Graphical Passwords. ACM Symposium on Usable Privacy and Security (SOUPS) (29% accept rate). ***Best Paper Award***

[C2] **S. Chiasson**, P.C. van Oorschot, R. Biddle (2006). A Usability Study and Critique of Two Password Managers. USENIX Security Symposium (12% accept rate). *[A*]*

[C1] **S. Chiasson**, and C. Gutwin (2005). Testing the Media Equation with Children, ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) (25% accept rate). *[A*]*

**Other refereed contributions (peer-reviewed workshop papers)**

[W13] **L. Kyi,** S. Chiasson, E. Stobert (2020). How Individual Differences Impact Perceived Password Security Management. USENIX WAY workshop (4-page paper).

[W12] **H. Assal**, S. Chiasson (2018). Motivations and Amotivations for Software Security: Preliminary Results. Workshop on Security Information Workers (WSIW), USENIX SOUPS.

[W11] **R. Mohamed,** S. Chiasson (2018). Digital aging for increasing privacy in Online Social Networks. Moving Beyond a "one-size-fits-all" approach: Exploring Individual Differences in Privacy Workshop, ACM CHI.

[W10] **H. Assal**, S. Chiasson (2014). Tor for All: A Usability Study of Tor-enabled Mobile Apps. GRAND NCE Annual Conference.

[W9] **S. Maqsood**, S. Chiasson, A. Girouard (2014). A First Exploration of a Gesture Based Authentication Scheme for Flexible Displays. GRAND NCE Annual Conference

[W8] **L. Zhang-Kennedy**, S. Chiasson, R. Biddle (2013). Interactive Comics as Visual Narratives in Computer Security Education. GRAND NCE Annual Conference.

[W7] S. Egelman, J. Bonneau, S. Chiasson, D. Dittrich, S. Schechter (2012). It's not stealing if you need it: A panel on the ethics of performing research using public data of illicit origin. Financial Cryptography and Data Security (FC), pp 124-132, Springer

[W6] **A. Fry**, S. Chiasson, A. Somayaji (2012). Not Sealed But Delivered: The (Un)Usability of S/MIME Today, Annual Symposium on Information Assurance (ASIA), pp. 48-61.

[W5] S. Chiasson (2011). Roundtable Discussion: Design and Teaching Considerations For E-Learning and Usable Security, AACE Conf. on E-Learning in Corporate, Government, Healthcare & Higher Education (E-LEARN) (4-pages)

[W4] **S. Chiasson, A. Forget**, R. Biddle (2008). Accessibility and Graphical Passwords. Symposium on Accessible Privacy and Security (SOAPS) (3-page paper on workshop website).

[W3] **S. Chiasson**, R. Biddle, A. Somayaji (2007). Even Experts Deserve Usable Security: Design guidelines for security management systems. Workshop on Usable IT Security Management, Pittsburgh, USA (4-page paper on workshop website).

[W2] **S. Chiasson**, R. Biddle (2006). Issues in User Authentication. ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) Workshop on Security User Studies Methodologies and Best Practices.

[W1] **S. Chiasson**, R. Biddle, P.C. van Oorschot (2006). Materials for a Usability Study of Password Managers. Security User Studies Workshop, ACM SOUPS.

**Other refereed contributions (peer-reviewed extended abstracts)**

[E30] **K. Chaudhry, A. Mann**, H. Assal, and S. Chiasson (2022). "I didn't even want to turn my head because I was so scared of the prof: Student perceptions of e-proctoring software" USENIX SOUPS (4-page paper, poster). ***Best Poster Award.***

[E29] F. Westin, K. Hundlani. S. Chiasson (2021). "I'll throw in a courtesy like": A poster about features, etiquette, and user privacy. USENIX SOUPS (4-page paper, poster). ***Best Poster Award.***

[E28] **M. Lutaaya, K. Baig, S. Maqsood,** S. Chiasson (2021). "I'm Not a Millionaire": How Users' Online Behaviours and Offline Behaviours Impact Their Privacy. ACM SIGCHI Conference on Human Factors in Computing Systems Late Breaking Work (CHI LBW) (7-page paper in ACM DL, poster).

[E27] **D. Napoli, S. Navas Chaparro,** S. Chiasson, E. Stobert (2020) Something Doesn't Feel Right: Using Thermal Warnings to Improve User Security Awareness, USENIX SOUPS (4-page paper, poster).

[E26] **D. Napoli,** S. Chiasson (2019) Security Implications of Online Accessibility Obstacles for Users with Visual Impairments, USENIX SOUPS (5-page paper on SOUPS website, poster)

[E25] **D. Napoli**, S. Chiasson (2018) Assessing Non-Visual SSL Certificates with Desktop and Mobile Screen Readers, ACM CCS Extended Abstracts (2-page paper in ACM DL, poster)

[E24] **S. Maqsood, S. Maqsood**, R. Biddle, and S. Chiasson (2018). An Exploratory Study of Children's Online Password Behaviours. ACM IDC Extended Abstracts. (6-page paper in ACM DL, poster).

[E23] **D. Napoli**, S. Chiasson. Exploring the Impact of Colour-Blindness on Computer Game Performance. ACM CHI Late Breaking Work (6-page paper in ACM DL, poster).

[E22] **D. Napoli** (2018). Developing Accessible and Usable Security (ACCUS) Heuristics. ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) Student Research Competition (SRC) (6-page paper in ACM DL, poster).

[E21] **M. Lutaaya** (2018). Rethinking App Permissions on iOS. ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) Student Research Competition (SRC) (6-page paper in ACM DL, poster).

[E20] **S. Maqsood** (2018). Evaluation of a Persuasive Digital Literacy Game for Children. ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) Student Research Competition (SRC) (6-page paper in ACM DL, poster).

[E19] **L. Zhang-Kennedy**, R. Biddle, S. Chiasson (2017). Secure Comics: An Interactive Comic Series for Improving Cyber Security and Privacy. British HCI Interactions Gallery (2-page paper in conference proceedings)

[E18] **L. Zhang-Kennedy**, S. Chiasson (2016). Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge (ACM IDC) (poster, 6-page paper)

[E17] **M. Lutaaya**, S. Chiasson (2015). Password Rehearsal Memory Games. Symposium on Usable Privacy and Security (SOUPS) (poster, 2-page paper on conference website).

[E16] **L. Zhang-Kennedy, E. Fares**, S. Chiasson, R. Biddle (2015). Geo-Phisher: The design of a global phishing trend visualization. Symposium on Usable Privacy and Security (SOUPS) (poster, 2-page paper on conference website).

[E15] **H. Assal, J. Wilson**, S. Chiasson, R. Biddle (2015). Collaborative Security Code-Review: Towards Aiding Developers. Symposium on Usable Privacy and Security (SOUPS) (poster, 2-page paper on conference website).

[E14] **H. Assal**, S. Chiasson (2014). Will this onion make you cry? A usability evaluation of Tor-enabled mobile apps. Symposium on Usable Privacy and Security (SOUPS), (2-page paper on conference website). Distinguished Poster Award

[E13] **C. Mekhail, L. Zhang-Kennedy**, S. Chiasson (2014). Visualizations to Teach about Mobile Online Privacy. Persuasive Technology Conference, (2-page paper in Springer LNCS, poster).

[E12] **S. Maqsood** (2014). Shoulder Surfing Susceptibility of Bend Passwords. ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) Student Research Competition (SRC) (6-page paper in ACM DL, poster).

[E11] **S. Maqsood**, S. Chiasson, A. Girouard (2013). Passwords on Flexible Display Devices. ACM CCS (3-page paper in ACM DL, poster).

[E10] **E. Stobert**, S. Chiasson, R. Biddle (2011). User-Choice Patterns in PassTiles Graphical Passwords. ACSAC (2-page paper, poster).

[E9] S. Chiasson, **C. Deschamps, M. Hlywa, G. Chan, E. Stobert**, R. Biddle (2010). MVP: A web-based framework for user studies in authentication. ACM SOUPS, (2-page paper in ACM DL, poster).

[E8] **E. Stobert**, S. Chiasson, R. Biddle (2010). Persuasion, Social Graces, and Computer Security. PERSUASIVE 2010, Springer LNCS (4-page paper in proceedings, poster).

[E7] **A. Forget**, S. Chiasson, R. Biddle (2010). Input Precision for Gaze-Based Graphical Passwords. ACM CHI (6-page paper in ACM DL, Work-in-Progress (WIP) poster).

[E6] **A. Forget**, S. Chiasson, R. Biddle (2009). Lessons from Brain Age on Persuasion for Computer Security. ACM CHI (6-page paper in ACM DL, Work-in-Progress (WIP) poster).

[E5] **A. Forget**, S. Chiasson, R. Biddle (2008). Lessons from Brain Age on Password Memorability. ACM Future Play (2-page paper in ACM DL, poster).

[E4] **D. LeBlanc, S. Chiasson**, A. Forget, R. Biddle (2008). Can eye gaze predict graphical passwords? ACM SOUPS (2-page paper on conference website, poster).

[E3] **A. Forget, D. Arnold**, **S. Chiasson** (2007). CASE-FX: Feature Modeling Support in an OO CASE Tool. ACM OOPSLA (2-page paper in ACM DL, poster).

[E2] **A. Forget, S. Chiasson**, R. Biddle (2007). Helping Users Create Better Passwords: Is this the right approach? ACM SOUPS (2-page paper on conference website, poster).

[E1] **A. Forget, S. Chiasson**, R. Biddle (2007). Helping Users Protect Themselves from e-Criminals in Click-Based Graphical Passwords. APWG eCrime Summit, (2-page paper, poster).

**Non-refereed contributions (technical reports)**

[TR2] **L. Zhang-Kennedy**, S. Chiasson, R. Biddle (2014). Using comics to teach about mobile online privacy. Technical Report TR-14-02, School of Computer Science, Carleton University.

[TR1] **S. Chiasson** and C. Gutwin (2005). Design Principles for Children's Software, Technical Report HCI-TR-05-02, Computer Science Department, University of Saskatchewan, Saskatoon, Canada.

**Non-refereed contributions (invited or minimally reviewed)**

[N19] **M. Shlega,** S. Maqsood, S. Chiasson (2022). Users, Smart Homes, and Digital Assistants: Impact of Technology Experience and Adoption. HCI International (HCII) (paper).

[N18] **D. Napoli, S. Navas Chaparro**, S. Chiasson (2021). Enhancing the Experience of Security and Privacy Warnings with Smell, Taste, and Temperature. ACM CHI Workshop on Smell, Taste, and Temperature Interfaces (STT) (position paper)

[N17] **L. Zhang-Kennedy**, S. Chiasson (2015). Improving Children's Mobile Privacy Awareness and Behaviour. SOUPS Workshop on Inclusive Privacy and Security (WIPS) (position paper).

[N16] **S. Hurtado**, S. Chiasson (2015). Unfamiliar road signs: Measuring the impact on driver distraction. CRA-W Graduate Cohort Workshop (poster).

[N15] **M. Baslyman**, S. Chiasson (2015). "Smells Phishy": An Educational Game About Online Phishing Scams. University of Ottawa Annual Engineering and Computer Science Poster Competition. (poster) ***IEEE Best Poster Award (first place out of 65 entries).***

[N14] **G. Reynaga**, S. Chiasson (2014). Adapting CAPTCHAs for Smartphone Usage. NSERC Surfnet Newsletter, v5(1).

[N13] A. Forget, S. Chiasson, R. Biddle (2014). Towards supporting a diverse ecosystem of authentication schemes. SOUPS Who Are You?: Adventures in Authentication: WAY Workshop (2-page paper)

[N12] **S. Hurtado, A. Imran**, S. Chiasson (2014). A usability study of ChatSecure. CRA-W Graduate Cohort Workshop (poster).

[N11] **S. Maqsood**, S. Chiasson, A. Girouard (2014). Bend passwords for flexible displays. CRA-W Graduate Cohort Workshop (poster).

[N10] **L. Zhang-Kennedy, C. Mekhail**, S. Chiasson (2014). Visualizations to teach about mobile online privacy. GRAND NCE Annual Conference (poster).

[N9] **V. Boothroyd**, A. Patrick, S. Chiasson (2014). Older adults' perception of online risk. GRAND NCE Annual Conference (poster).

[N8] **L. Zhang-Kennedy**, S. Chiasson, R. Biddle (2013). Interactive comics to teach about computer security. GRAND NCE Annual Conference (poster).

[N7] **V. Boothroyd**, S. Chiasson (2013). Perception of online risk: How do older and younger adults perceive online risk? NSERC ISSNet Annual Workshop (poster).

[N6] **S. Maqsood**, S. Chiasson (2013). Passwords on Flexible Display Devices. NSERC ISSNet Annual Workshop (poster).

[N5] **Y. Xu, G. Reynaga**, S. Chiasson, J.M Frahm, F. Monrose, P.C. van Oorschot. (2012) Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion. ACM SOUPS (poster).

[N4] **L. Zhang**, S. Chiasson, R. Biddle (2012). Teaching about Password Guessing Attacks Through Visualizations. GRAND NCE Annual Conference (poster).

[N3] **V. Boothroyd**, S. Chiasson. (2012). Writing down your password: Does it help? NSERC ISSNet Annual Workshop (poster).

[N2] **H.-Y. Chiang**, S. Chiasson. (2012). Usability testing of graphical password schemes on mobile devices. NSERC ISSNet Annual Workshop (poster).

[N1] **S. Chiasson** and R. Biddle (2007). Persuading Users to Behave Securely. Persuasive Technology (poster).

## 4. Evidence of Impact, Contributions, and Leadership

### Awards and Distinctions

(2022) Research Excellence Award, Faculty of Science, Carleton University
(2022) NSERC Prize: Arthur. B. McDonald Fellowship (one of six awarded nationally)
(2022) Best Poster award, USENIX Symposium on Usable Privacy and Security (SOUPS)
(2021) Honorable Mention Award, ACM SIGCHI Conference on Human Factors in Computing System (CHI) (awarded to top 5% of papers)
(2021) Best Poster award, USENIX Symposium on Usable Privacy and Security (SOUPS)
(2021) Carleton Research Achievement Award
(2019) Best Paper Award, ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) (awarded to top 1% of papers)
(2019) Carleton Student Support Certificate. Completed 15-hour series of workshops on how to more effectively support students (Communication, referrals, indigenous cultural awareness, cross-cultural competence, sexual violence response, supporting students in distress, Safer Spaces LGBT+ support)
(2017) NSERC Discovery Accelerator Supplement, awarded to researchers with superior research programs in terms of originality and innovation, and showing strong potential to become international leaders in their field.
(2017) Carleton Faculty Graduate Mentoring Award, awarded yearly to 1% of faculty from nominations by past and current graduate students.
(2017) Canada Research Chair in User-Centric Cybersecurity, Tier 2
(2016) One of six researchers invited to the Young Leading Scientists dinner meeting hosted by Minister Duncan, the Federal Minister of Science.
(2016) Honorable Mention for Best Paper award for the APWG/IEEE eCrime conference
(2016) Emerald Literati Network Award for Excellence for the journal paper "User-centred authentication feature framework"

(2016) Canadian Women in Computing Conference (CWiC) Poster Competition, 3rd place (student: Sana Maqsood)
(2015) IEEE Best Poster Award (student: Malak Basylman), University of Ottawa poster competition (first place out of 65 entries).
(2014) Carleton Graduate Student Association's Excellence Award in Graduate Teaching
(2014) Distinguished Poster Award (student: Hala Assal), SOUPS Conference.
(2014) One of ten papers nominated for a SOUPS Impact Award (Paper: A second look at the usability of click-based graphical passwords)
(2013) Nominated for a Carleton Faculty Graduate Mentoring Award by past and current graduate students.
(2012) Canada Research Chair in Human-Oriented Computer Security, Tier 2.
(2012) Honorable mention Poster Award (student: Vanessa Boothroyd), ISSNet Workshop
(2012) Finalist for Best Paper award for the APWG/IEEE eCrime conference.
(2009) Carleton Senate Medal for Outstanding Academic Achievement
(2009) Finalist, Ottawa Centre for Research and Innovation (OCRI) Student Researcher of the Year
(2008) One of six PhD students selected internationally to present research at the Google Workshop for Women in Engineering, San Jose, CA
(2008) Ontario Graduate Scholarship in Science and Technology (OGSST) (awarded but declined)
(2007) Best Paper Award for the Symposium on Usable Privacy and Security (SOUPS)
(2006, 2007) Hendrika Alice Eisen Memorial Scholarship
(2000) Represented Canada at the IFIP World Computer Congress's Youth Forum in Beijing

**Invited Talks and Panels**

[S55] (2022) Panelist, #BreakTheBias in Science, Carleton University, virtual
[S54] (2021) Invited speaker, Designing for when humans and cybersecurity interact, Lakehead University, December 2021, virtual
[S53] (2021) Invited speaker, When humans and cybersecurity interact, WiCyS, University of Windsor, October 2021, virtual
[S52] (2021) Keynote speaker, International Conference on Availability, Reliability, and Security (ARES), August 2021, virtual
[S51] (2021) Invited speaker, The challenge of designing for security and privacy, York University, virtual
[S50] (2019) Panelist, Cybersecurity Policy Crunch, Institute on Governance, Ottawa
[S49] (2019) Guest lecture, HCIN5100, Designing for children, Carleton, Ottawa
[S48] (2019) Invited speaker, Usable Authentication, NERD.nrw Summer School, Aachen, Germany
[S47] (2019) Panelist, Preparing for the Future, Project Tech Conference, Ottawa
[S46] (2019) Invited speaker, End-user Cybersecurity, SHAD high school students, Carleton, Ottawa
[S45] (2019) Invited speaker, Computer security advice you can actually use, Discovery Café lecture series, Ottawa
[S44] (2018) Invited speaker, Children and online safety, Carleton's Science Café, Ottawa
[S43] (2018) Invited speaker, Fostering a security mindset. Centre for National Security, Conference Board of Canada, Ottawa.
[S42] (2018) Invited speaker, End-user Cybersecurity, SHAD high school students, Carleton, Ottawa
[S41] (2018) Invited speaker, Staying safe online: exploring cyber threats and protection strategies, Digital Inclusion Week, Ottawa Public Library.
[S40] (2018) Invited speaker, Women in Science and Engineering, Ottawa Chapter.
[S39] (2017) Keynote, Achieving practical security by acknowledging human users, Annual Summit for Information Technology Governance and Security, ISACA, Montreal.
[S38] (2017) Invited speaker, Achieving practical security by acknowledging human users, McMaster University.

[S37] (2017) Panelist, "Faculty Panel: What I wish someone had told me in my first year…", New Faculty Orientation, Carleton University.
[S36] (2017) Invited speaker, End-user Cybersecurity, SHAD high school students, Carleton, Ottawa
[S35] (2017) Panelist, Canada's Cyber R&D Agenda, CyberNB, Fredericton
[S34] (2017) Panelist, Leveraging Emerging Technologies to Benefit Canadians, Research Money Annual Conference, Ottawa
[S33] (2017) Expert Contributor, Security Leadership, Canadian Security & Intelligence Leadership Program, University of Ottawa
[S32] (2017) Expert commentary, Designing Privacy for Real People Symposium, Rotman School of Management, University of Toronto
[S31] (2017) Invited speaker, Eyetracking: insight into user behaviour, About the User lecture series, 1125@Carleton, Ottawa
[S30] (2017) Panelist, User Decision-Making, USEC, San Diego
[S29] (2017) Panelist, Meaningful Consumer Adoption Challenges and Solutions, Digital Adoption Symposium, Ottawa
[S28] (2017) Invited speaker, Staying safe online: exploring cyber threats and protection strategies, Carleton's Science Café, Ottawa
[S27] (2016) Invited speaker, Improving Children's Mobile Privacy Awareness and Behaviour, Privacy Education Project, Canadian Civil Liberties Association, Toronto
[S26] (2016) Invited speaker, Understanding users' (in)secure behaviour, Cyber Summit, Banff, AB
[S25] (2016) Invited speaker, Recommendations for usable security, Intergovernmental Forum on Risk Management, Conference Board of Canada, Ottawa
[S24] (2016) Invited speaker, Research lessons from the last 5 years. Passion for Research Luncheon, Carleton University, Ottawa
[S23] (2016) Invited speaker, Security & Privacy, SHAD high school students, Carleton, Ottawa
[S22] (2016) Invited speaker, Designing for security: users are not the weakest link, Open Web Application Security Project (OWASP), Ottawa Chapter
[S21] (2016) Invited speaker, Recommendations for usable security, Internal Audit Services, Employment and Social Development Canada, Government of Canada, Ottawa
[S20] (2016) Invited speaker, Understanding users' (in)secure behaviour, Colgate University, NY
[S19] (2016) Invited speaker, Designing for security, Cyber Security: The Human Factor conference, Conference Board of Canada, Ottawa ON
[S18] (2016) Invited speaker, User authentication for children, Canadian Internet Registration Authority (CIRA)
[S17] (2015) Invited speaker, Users are not the weakest link, ETH Zurich, Switzerland
[S16] (2015) Invited speaker, Designing for security, Middlesex University, London, UK
[S15] (2015) Invited speaker, Security & Privacy, SHAD high school students, Carleton, Ottawa
[S14] (2015) Invited speaker, Researcher perspectives, Information and Communications Technology Council (ICTC), Virtual Community of Practice for Digital Adoption
[S13] (2015) Invited speaker, Understanding users' (in)secure behaviour, University of California at Berkeley, CA
[S12] (2015) Invited speaker, Information visualization for influencing secure behavior, Office of the Privacy Commissioner of Canada
[S11] (2014) Invited speaker, Usable Security, Concordia University, Montreal
[S10] (2014) Panelist, Faculty of Science annual alumni panel, Carleton
[S9] (2013) Invited speaker, Mental Models of Computer Security, TU Darmstadt, Germany
[S8] (2013) Guest lecture Persuasive Technology, computer science graduate class, Carleton
[S7] (2012) Panelist, Ethics of using Stolen Datasets panel, Workshop on Ethics in Computer Security Research, co-located with Financial Cryptography and Data Security, Bonaire
[S6] (2012) Guest lecture, The Media Equation and Persuasive Technology, computer science graduate class, Carleton

[S5] (2012) Guest lecture, Usable Security, in 3rd year undergraduate class, Carleton
[S4] (2012) Invited speaker, Usable Security, Research in Motion, Waterloo
[S3] (2012) Invited speaker, Usable Security, University of Waterloo
[S2] (2012) Invited speaker, Usable Security, Université du Québec en Outaouais, Gatineau
[S1] (2011) Invited speaker, Usable Security, Association de Sécurité de l'Information du Montréal Métropolitain

**Chairing and Organization**

(2020 – 2022) General Chair, USENIX Symposium on Usable Privacy and Security (SOUPS)
(2019, 2018) Technical Program Co-Chair, SERENE-RISC Fall Cybersecurity Workshop (2 days)
(2021, 2019, 2018) Co-Chair, CLUE Symposium on Human-Computer Interaction (1 day)
(2018, 2017) Technical Program Co-Chair, Symposium on Usable Privacy and Security (SOUPS)
(2017 - 2023) Steering Committee, USENIX Symposium on Usable Privacy and Security (SOUPS)
(2017) Co-Chair, Examining cybercrime: SME edition, 2-day workshop for SERENE-RISC and GoSec Annual Conference
(2017) General Chair, Spring Cybersecurity Workshop, SERENE-RISC (2 days)
(*2019*, 2018, 2017, 2015, 2014, 2012, 2010) Co-organizer, HCI Workshop, SHAD, Carleton University
(2016) General Chair, Fall Cybersecurity Workshop, SERENE-RISC (2 days)
(2016) Chair, Examining cybercrime: financial edition, workshop for SERENE-RISC and APWG
(2015) Chair, Examining cybercrime, full-day workshop for SERENE-RISC and SOUPS (2015)
(2015) Chair, Local Arrangements, SOUPS (2015)
(2014, 2013) Chair, Tutorials and Workshops, SOUPS
(2013, 2012) Co-chair, Usable Privacy & Security for Mobile Devices Workshop (U-PriSM)
(2012) Chair, ISSNet Workshop on Mobile Security and Privacy
(2012, 2011) Co-chair, Poster Session, SOUPS
(2011) Co-instructor, Experiment Design and Quantitative Methods for Usable Security Research. Half-day tutorial for SOUPS
(2011) Co-chair, The Future of User Authentication and Authorization on the Web Workshop, co-located with Financial Cryptography and Data Security (FC)
(2010) Tutorial instructor, Introduction to Usable Security, for IEEE Privacy, Security, Trust (PST)
(2010) Co-chair, User Studies Experience Report (USER) Workshop, co-located with SOUPS
(2010) Co-chair, Poster Session, NSERC ISSNet Annual Workshop
(2009) Co-instructor, HCI Methodology and Usable Security. Full-day tutorial for NSERC ISSNet

**Editorial Board**

(2021) Associate Editor, ACM Transactions on Computer Human Interaction (TOCHI)

**Program Committees**

(2021) Graphics Interface (GI)
(2019, 2012) Financial Cryptography and Data Security (FC)
(2019) USENIX Enigma
(2019, 2018, 2017, 2016, 2015, 2014, 2012, 2011) Symposium on Usable Privacy and Security (SOUPS)
(2017, 2016, 2015) Workshop on Usable Security (USEC)
(2016) European Workshop on Usable Security (EuroUSEC)
(2014) Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)
(2014) ACM Symposium on Access Control Models and Technologies (SACMAT)
(2014) Grace Hopper Celebration of Women in Computing Conference, Security & Privacy track
(2014) Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)
(2013) IEEE Privacy, Security, and Trust (PST)
(2013-Deputy Chair, 2012, 2011) USENIX Security

(2013) IFIP INTERACT
(2012) International conference on Trust and Trustworthy Computing (TRUST)
(2010) British HCI

**Relevant Carleton University Committees**

(2023 – ) Governance committee, Collaborative specialization in accessibility
(2022 – ) Faculty of Science EDI research committee
(2023) Research Achievement Award adjudication committee
(2022) Graduate Administrator hiring committee, School of Computer Science
(2021 – 2022) Chair, Faculty hiring committee (HCI), School of Computer Science
(2021 – 2022) School of Computer Science Executive Committee
(2020 – ) School of Computer Science Equity, Diversity, Inclusion committee
(2021, 2019, 2016, 2015, 2013) Faculty hiring committee, School of Computer Science
(2014 – 2017, 2018 – 2022) University Research Ethics Board (CUREB-B) committee
(2019, 2020) Tenure and Promotion Committee, School of Computer Science
(2016 – ) Carleton representative for Canada's Cyber Security Challenge (CyberSci)
(2015 – ) Faculty member of the Women in Computer Science committee
(2020) Faculty hiring committee, Systems and Computer Engineering
(2020) CRC in Data Science hiring committee, Faculty of Science
(2020) Faculty Graduate Mentoring Award selection committee
(2020) SCS Director selection advisory committee, Faculty of Science
(2014 – 2016) Graduate Studies committee, School of Computer Science

**Expert Assessment and Reviewing Activities**

(2021) NSERC Discovery Grant, external reviewer
(2021, 2016, 2013, 2011) Reviewer, Luxembourg National Research Fund (FNR) grant proposal
(2021, 2016, 2014) MITACS Accelerate grant reviewer
(2020) NSERC Alliance Grant reviewer
(2020) SOUPS Impact Award Committee
(2018) External reviewer, tenure and promotion, Université de Montréal
(2018) External reviewer, tenure and promotion, University of Waterloo
(2018) Judge, Canada Wide Science Fair, Ottawa
(2017) Site Visit Committee, NSERC Collaborative Research and Development Grants (CRD)
(2017) ACM SIGSAC Awards Selection Committee (Outstanding Innovation Award and Outstanding Contributions Award)
(2017) Reviewer, Canada Research Chairs program
(2017) Expert consultation, ranking of publication venues for usable security, Computer Science Department, Brigham Young University
(2016) Jury member, SSHRC Human Dimensions Open Data Challenge, in collaboration with Compute Canada, Ontario Centres of Excellence, and ThinkDataWorks
(2015) Reviewer, NSERC Collaborative Research and Development Grants
(2013) External reviewer, Canada Research Chair candidate application at the university level
(2011, 2010) Reviewer, Computer Security course materials, Computer Science Department, Western Illinois University. Course developed as part of a grant from the NSF-CCLI Program
(**on-going**) *Journal reviewing*: Computers & Security, Trans. on Information and System Security (TISSEC), Jour. of Systems and Software (JSS), Oxford's The Computer Journal, Trans. on Dependable and Secure Computing (TDSC), Interacting with Computers (IwC), Comm. of the ACM (CACM), IET Information Security, International Journal of Human-Computer Studies, Journal of Internet Services and Applications, IEEE Transactions on Information Forensics and Security (TIFS), IEEE Trans. On Human-Machine Systems (THMS), Behaviour & Information Technology, Int. Journal on Human Computer Interaction (IJHCI), Computer Supported Cooperative Work (COSU), IEEE Internet Computing, Transactions on Computer-Human Interaction (TOCHI)
(**on-going**) *Conference Reviewing*: ACM Computer Human Interaction (CHI), ACM Graphical Interfaces (GI), British Human Computer Interaction (BCS-HCI), ACM Designing Interactive Systems (DIS), ACM

Tangible, Embedded, and Embodied Interaction (TEI), ACM Computer and Communications Security (CCS), SECRYPT, ACM MobileHCI, International Conference on Pervasive Computing (PERVASIVE), INTERACT, Interaction Design and Children (IDC)

**Research Networks**

(2021 – 2026) Human-Centric Cybersecurity (H2C) Partnership (SSHRC)
*Behavioural Cluster Coordinator, Project Leader, EDI Champion, Co-investigator*

(2020 – ) National Cybersecurity Consortium (NCC)
*Co-investigator* in the Human Centric Cybersecurity Network

(2016 – ) *Collaborator,* International Centre for Comparative Criminology, Université de Montréal

(2014 – 2021) SERENE – Smart Cybersecurity Network
Networks of Centers of Excellence – Knowledge Management (NCE-KM).
Scientific Director: Benoit Dupont, Criminology, Université de Montréal
*Acting Scientific Director (2016-17), Deputy Scientific Director: Sonia Chiasson, Computer Science, Carleton University*

(2012 – 2015) NSERC Surfnet Strategic Network - *Collaborating Researcher*

(2011 – 2015) GRAND Network of Centres of Excellence
*Collaborating Network Investigator (CNI), PSAWARE sub-project leader*

(2010 – 2014) NSERC Internetworked Systems Security Network (ISSNet) Strategic Network
*Project Leader for Human Behaviour and Computer Security Project and Co-PI*

## 5. Training of HQP

I currently supervise 2 PhD students, 5 Masters students, 3 undergraduates, and 2 additional research assistants.

| | **Completed** | **In-progress** |
|---|---|---|
| **Graduate** | 6 PhD, 26 Masters | 2 PhD (+1 incoming), 1 Masters (+ 3 incoming) |
| **Undergraduate** | 16 completed | 1 in progress |

### Graduate Supervision Completed

**Postdoc**

1. 2020 – 21 Sana Maqsood, Computer Science (Tenure-track faculty York University – July 2022)

**PhD Completed**

6. 2015 – 20 Sana Maqsood, PhD(CS), *The design, development, and evaluation of a digital literacy game for preteens*. awarded MITACS 3-year PhD Fellowship. Game deployed in over 400 Canadian schools. Currently Tenure-track assistant professor at York University.

5. 2015 – 19 Riham Mohamed, PhD(CS), *Investigating Decay Representations for Privacy and Online Reputation Management.* awarded a 4-year Ontario Trillium Scholarship, NSERC CREATE/CLUE internship with Trend Micro June – October 2016, IRCC Jan-Apr 2018. Currently employed at IRCC.

4. 2013 -- 18 Hala Assal, PhD(CS), *The Human Dimension of Software Security and Factors Affecting Security Processes,* awarded NSERC PGS-D scholarship. Awarded 2018 Senate Medal for Outstanding Academic Achievement. Currently Tenure-track assistant professor at Carleton University.

3. 2013 – 17 Leah Zhang-Kennedy, PhD(CS), *Multimedia Approaches for Improving Children's Privacy and Security Knowledge and Persuading Behaviour Change,* awarded OGS graduate scholarship. Currently Tenure-track assistant professor at University of Waterloo Stratford Campus.

2. 2011 - 15 Gerardo Reynaga, PhD(CS), *The usability and security of captchas on mobile devices* (co-supervised with Paul van Oorschot starting in 2011). Currently employed at Sabre Airline Solutions.

1. 2009 - 12 Alain Forget, PhD(CS), *A world with many authentication schemes* (co-supervised with Robert Biddle). Awarded 2013 Senate Medal for Outstanding Academic Achievement. Post-doctoral fellow at Carnegie Mellon University, now employed at Google.

**Masters Completed**

| | | |
|---|---|---|
| 26. | 2021 – 23 | Maxwell Keleher, MCS(HCI), *Exploring Privacy Implications of Devices as Social Actors*, QEII scholarship, *nominated for Senate Medal* |
| 25. | 2021 – 23 | Sami Ortiz Huayhua, MA(HCI), *TikTok, privacy, and young adults,* co-supervised with Robert Biddle |
| 24. | 2020 – 23 | Svetlana Dobrynina, MA(HCI), *Understanding Mental Models of Password Managers,* co-supervised with Elizabeth Stobert |
| 23. | 2020 – 23 | Khadija Baig, MCS, *Privacy, biological relatives, and at-home DNA testing* |
| 22. | 2020 – 23 | Ashi Mann, MA(HCI), *Investigating factors relating to fear, uncertainty, and doubt (FUD) in end-user cryptocurrency behaviours.* |
| 21. | 2018 – 20 | Fiona Westin, MA(HCI), *FoMO-Centricity: How social media's dark designs cause users to reluctantly give up their data*. CREATE/CLUE internship |
| 20. | 2016 – 20 | Sandra Gabriele, MASc(HCI), *User awareness of privacy risks related to the collection of fitness tracker data.* |
| 19. | 2017 – 19 | Jessica Rocheleau, *Privacy Attitudes and Behaviours of Autistic and Non-Autistic Teenagers on Social Networking Sites*, MA(HCI), NSERC CREATE/CLUE internship, SSHRC-CGS-M scholarship. Awarded 2019 Senate Medal for Outstanding Academic Achievement. |
| 18. | 2018 – 19 | Navneet Sidhu, *Interactive Educational tool for Fitness Trackers,* MCS project |
| 17. | 2017 – 19 | Michael Lutaaya, MCS, *Me, Myself, and ID: Towards Usable, Privacy-Preserving, Fraud-Resistant Digital Identity Services for Smartphone Users,* NSERC CGS-M scholarship |
| 16. | 2016 – 19 | Rebecca Jeong, MASc(HCI), *Children and adults' perception of signal colours, symbols, and words in the context of cybersecurity warnings*, (started supervision July 2017), NSERC CREATE/CLUE Internship |
| 15. | 2016 – 18 | Yomna Abdelaziz, MASc(HCI), *Responsibility, Trust, and Monitoring Tools for End-User Account Security*, NSERC CREATE/CLUE internship at TrendMicro. Currently employed at IBM. |
| 14. | 2016 – 18 | Daniela Napoli, MA(HCI), *Accessible and Usable Security: Exploring Visually Impaired Users' Online Security and Privacy Strategies*, NSERC CREATE/CLUE internship with CAE |
| 13. | 2015 – 18 | Sumbal Maqsood, MCS(HCI), *Children's Text Password Behaviors and Parental Advice* (co-supervised with R. Biddle). Currently employed with Gov. of Canada. |
| 12. | 2014 – 16 | Kalpana Hundlani, MCS, *A parent-child password manager*. Co-op internship with Caseware May – Dec 2015. |
| 11. | 2014 – 16 | Christine Mekhail, MASc(HCI), *"A day in the life of the Jos": The design of an educational game on privacy*. MITACS internship with MediaSmarts Jun – Oct 2015, NSERC CREATE internship with Canadian Intellectual Property Office |
| 10. | 2013 – 15 | Stephanie Hurtado, MCS, *An eye-tracking evaluation of driver distraction and road signs,* coop with Blackberry Apr 2014-Dec 2014. |
| 9. | 2014 – 15 | Vikas Nagaraj, MIPIS, started in Sept 2012 (part-time), agreed to supervise in Apr 2014, *Information visualization for detecting suspicious key signing activities*. Project-based Masters**.** |

8. 2012 – 15 Derek Wueppelmann (part-time), MCS(HCI), *PGP Auth: public key encryption for authentication on the web.*

7. 2013 – 15 Ahsan Imran, MCS, *A comparison of password authentication between children and adults*, coop with Espial Group Apr 2014-Dec 2014.

6. 2013 – 15 Matthew Hull, MA(HCI), *Factors affecting secure computer behaviour*. PhD student in cognitive science at Carleton.

5. 2012 - 14 Sana Maqsood, MCS(HCI), *Bend passwords: using gestures to authenticate on flexible displays* (co-supervised with Audrey Girouard). Nominated for a University medal.

4. 2013 - 14 Shuja Shahzada, MASc(HCI), *Touch interaction for user authentication* (co-supervised with Robert Biddle).

3. 2011 - 14 Vanessa Boothroyd, MA(HCI), *Older adults' perception of online risk* (co-supervised with Andrew Patrick).

2. 2011 - 13 Leah Zhang, MASc(HCI), *Improving mental models of computer security through information visualization* (co-supervised with Robert Biddle).

1. 2012 – 13 Hsin-Yi Chiang, MCS, *A graphical password scheme for mobile devices*.

**Graduate Supervision In-progress**

**PhD In-progress**

3. *2023 – 27* *Maxwell Keleher, PhD(CS) (incoming F2023), NSERC CGS-D*

2. 2019 – 23 Srivathsan G. Morkonda, PhD(CS), co-supervised with P.C. van Oorschot (switched to PhD Jan 20, awarded OGS

1. 2018 – 23 Daniela Napoli, PhD(CS), awarded QEII scholarship, OGS(declined), NSERC PGS-D

**Masters In-progress**

4. *2023 – 25* *Muhammad Zaid Arif, MHCI (incoming F2023)*

3. *2023 – 25* *Charlotte Carr, MHCI (incoming F2023)*

2. *2023 – 25* *Chanthea Quinland, MHCI, co-supervised with Elizabeth Stobert (incoming W2024)*

1. 2021 – 23 Kazma Chaudhry, MA(HCI), internship at CIHI

**Undergraduate Supervision – Honours projects/thesis**

20. 2023 *Sebastian Navas Chaparro, Computer Science, honour's thesis (Jan – Aug 2023),* ***2023 Provost Scholar Award***

19. 2022 Ketki Panse, Computer Science, honour's project, co-supervised with H. Assal. Surveying and understanding student experiences with e-proctoring

18. 2022 Erica Morgan, Computer Science, honour's thesis, The Usability of Mobile Cryptocurrency Wallets for First-TimeUsers; ***research presented at NCUR 2022***

| | | |
|---|---|---|
| 17. | 2021 | Cameron O'leary, Computer Science, honour's project, phishED: an anti-phishing educational website |
| 16. | 2021 | Monica Vu, Computer Science, honour's project, Proof of concept and exploration of a piano-based password scheme |
| 15. | 2022 | Shubham Sharan, Computer Science, honour's thesis, Effectiveness of a quiz user interface |
| 14. | 2022 | Paulina Chametka, Computer Science, honour's thesis, Perceptions of mental health chatbots; ***research presented at NCUR 2022*** |
| 13. | 2021 | Abdul Siddiqui, Computer Science, honour's project, Pinny: a mobile app for athletes looking for pickup games |
| 12. | 2020 | Kelvin Hua, Computer Science, honour's project, FoodBucket app |
| 11. | 2020 | Xinting Wang, honour's project, Computer Science, 2D Internet Security Educational Game |
| 10. | 2020 | Khadija Baig, Computer Science, Users' Perceptions of At-home DNA Testing Companies, ***Provost Scholar Award, research presented at NCUR 2021*** |
| 9. | 2018 | Michael Lutaaya, Computer Science, Proof-of-Concept Implementation of an Alternative iOS Permission Manager |
| 8. | 2017 | Matthew Penny, Computer Science, User Trust and Adherence toward Tiered Warning Messages in Web Browsers |
| 7. | 2014 | Carolyn Kenney, Computer Science, Exploring Gesture-Based Passwords with the Kinect System |
| 6. | 2013 | Cory Ling, Computer Science, Password Rehearsal Memory Games |
| 5. | 2013 | Nicholas Shires, Computer Science, Mobile Augmented Reality Game for Childhood Education |
| 4. | 2012 | Marek Menhart, Computer Science, Image Component Recognition as a Usable Password |
| 3. | 2012 | Sana Maqsood, Computer Science, Usable Password Strength Meter |
| 2. | 2012 | Murray Christopherson, Computer Science, Net-Warr: A game to combine social media, computer security and education |
| 1. | 2011 | Weinan Liu, Computer Science, A security analysis of information leakage in graphical password discretization methods |

**Research assistants and co-op students**

| | |
|---|---|
| 2022 | *LeeAnne King, Dean's Summer Research Internship (DSRI), co-supervised with S. Maqsood* |
| | *Kalumbu Kasaji, Dean's Summer Research Internship (DSRI), co-supervised with E. Stobert* |
| | Sebastian Navas Chaparro, research assistant, USRA summer student/coop |
| | Fiona Westin, research assistant |
| | Kalpana Hundlani, research assistant |
| 2021 | Preethi Nagabandi, Computer Science, Dean's Summer Research Internship (DSRI), |
| | Hamza Sohail, Computer Science, Dean's Summer Research Internship (DSRI) |
| | Michael Shlega, i-CUREUS research student |
| | Sebastian Navas Chaparro, i-CUREUS research student, USRA summer student/coop |
| | Fiona Westin, research assistant |
| | Kalpana Hundlani, research assistant |
| 2020 | Hamza Sohail, Computer Science, i-CUREUS summer student |
| | Sebastian Navas Chaparro, i-CUREUS research student, USRA summer student |

| | |
|---|---|
| | Cassandra Cassell, summer research assistant |
| | Kalpana Hundlani, summer research assistant |
| | Elisa Kazan, Computer Science research assistant |
| | Khadija Baig, Computer Science undergraduate research assistant |
| | Jeeheon Kim, Carleton Research Training Award |
| 2019 | Anna-Lena Theus, Communications, graduate research assistant |
| | Paulina Chatmetka, Computer Science coop student |
| | Sebastian Navas Chaparro, Computer Science undergraduate research assistant |
| | Sayrahoque Khan, Computer Science graduate research assistant |
| | Khadija Baig, Computer Science undergrad research assistant |
| 2017 | Jessica Rocheleau, HCI graduate research assistant |
| | Kalpana Hundlani, Computer Science research assistant |
| | Sandra Gabriele, HCI graduate research assistant |
| | Daniella Briotto Faustino, HCI graduate research assistant |
| 2016 | Khadija Baig, Computer Science undergraduate research assistant, coop student |
| | Michael Kuang, Computer Science Dean's Summer Research Internship (DSRI) |
| 2013 | Michael Lutaaya, Computer Science Dean’s Summer Research Internship (DSRI) |
| | Sarah Dorey, Interactive Multimedia & Design RA |
| 2012 | Simeon Robson Gordon, Computer Science co-op student |
| | Mickey Yuen, Computer Science co-op student |
| | Sara Lacelle, Cognitive Science undergraduate research assistant |
| 2011 | Manas Modi, IIT undergraduate summer internship |

**Graduate Thesis Committees**

**PhD**

2023 Eric Spero, PhD, Computer Science, User interfaces, mental models, and cybersecurity (Thesis examiner, April 2023)

2022 Yue Huang, PhD, Electrical and Computer Engineering, University of British Columbia, Toward Investigating Users' Understanding, Concerns, and Strategies Regarding Private Information Sharing (External examiner, November 2022)

2022 Eric Spero, PhD, Computer Science, Proposal defense (Thesis examiner, January 2022)

2017 Raof Moeini, PhD, Applied Linguistics and Discourse Studies. (PhD Advisory Committee)

Wahida Chowdhury, PhD, Cognitive Science. Online privacy versus online surveillance: Where do we draw the line? (Thesis examiner, April 2017)

Misagh Tavanpour, PhD, ECE, Upload User collaboration in the Data Upload for LTE-Advanced Networks (Thesis examiner)

2016 Derek Pasma, PhD, Cognitive Science, Carleton University (Thesis examiner)

2014 Elizabeth Stobert, PhD, Graphical Passwords and Practical Password Management (Proposal defense chair)

Alexander Verdonschot, PhD, Flips and Spanners (Proposal defense chair)

**Masters**

2023 Saman Karim, MCS, Exploring Accessibility and Companionship in Boardgames via Alexa (Thesis examiner, January 2023)

2021 Emine Sasal, MA HCI, An analysis on guidelines for persuasive interfaces on mobile applications (January 2022) (Thesis Examiner)

Norah AlJurba, MA HCI, The design of a wearable health device to monitor covid-19 outpatients (September 2021)(Defence Chair)

Nadia Markova, MA CogSci, Investigating concreteness fading in the programming domain (September 2021) (Thesis Examiner)

Lin Kyi, MA HCI, End-user mental models of social engineering attacks (July 2021) (Thesis Examiner)

2020 Joshua Carr, MA HCI, Evaluating the usability of PassThought Authentication (September 2020) (Defence Chair)

Zach Savelson, MA CogSci, The Impact of Student Emotions on Learning in a Productive Failure Paradigm (August 2020) (Thesis Examiner)

Eduardo Soto, MIT, Text Entry in Virtual Reality: Implementation of FLIK method and Text Entry Test-Bed (May 2020) (Thesis Examiner)

Vidhi Shah, MCS, User Acceptance of Online Tracking if 'Forgetting' was an Option (January 2020) (Thesis Examiner)

2019 Mohamed Al Sharnouby, MCS, Thread Homeostatis – real-time anomalous behavior detection using short sequences of messages for safety-critical software (September 2019) (Defence chair)

Lori Watanabe, MA, Alone with My Phone: Exploring Links Between Solitude, Technology Use, and Socio-Emotional Functioning in Adolescents (August 2019) (Thesis Examiner)

Zahra Hassanzadeh, MCS, User understanding of Internet Data Breaches (August 2019) (Thesis examiner)

Jordan Pollock, MASc(HCI). CountMarks: Multi-Finger Marking Menus for Mobile Interaction with Head-Mounted Displays (April 2019) (Thesis Examiner)

2018 Eric Spero, MA, A Non-Linear Electronic Textbook Format to Facilitate Deep Learning (Thesis examiner)

Daniella, Briotto Faustino MASc(HCI), Bend Passwords for People with Vision Impairment (Thesis examiner)

Anna-Lena Theus, MA(HCI), Does Context Matter? Investigating Factors Related to Students' Academic Achievement in Classroom and Online Courses (Thesis examiner)

Mahmut Erdemli, MA(HCI), Interactive Digital Mapping as a Park Planning Tool in the Creation of the Boucher-Forest Park in Gatineau, Quebec (Defense Chair)

Heather Qian, MCS(HCI), Empirical studies on selection and travel performance of eye-tracking in Virtual Reality (Thesis examiner)

Abdulrahman Alamoudi, MCS(HCI), Web-based semantic annotation tool for online multimedia learning content (Thesis examiner)

Maria G Celis Rangel, MCogSci, Investing The Impact Of An Incremental Mindset Intervention On Students? Beliefs And Programming Performance (Thesis examiner)

2017 Fayzah Alshammari, MCS, Towards an Evaluation of a Recommended Tor Browser Configuration in Light of Website Fingerprinting attacks, University of Ottawa (Thesis examiner)

Emily Walpole, MASc, An exploration of consumer expectations in video-based online consumer reviews (Thesis examiner)

Ioana Steau, MCS, Robot Fence-Jumping Search (Defense Chair)

Elias Fares, MASc(HCI) Paper Ninja: Effects of Bend Gesture Training on Learnability and Memorability in a Mobile Game (Thesis examiner)

Paden Shorey, MASc(HCI), An Exploration of In-Game Action Mappings with a Deformable Game Controller (Thesis examiner)

Crystal Sirard, MA(HCI), A Decision Support Tool for Problem Detection and Resolution in Healthy Newborns: An Exploratory Study to Understand Parental Acceptance and Perception of Usefulness (Thesis examiner)

2016 Peter Simonyi, MCS, Interaction support for web applications (Thesis examiner)

2015 Maya Lourenco Levin, MDes, Wearable Technology, Ubiquitous Computing, and Sport Performance: A User-Centred Design Approach to Framing Communication in Football (Thesis examiner)

Jeff Wilson, MCS, ACH Walkthrough: Designing and building a web application for collaborative sensemaking (Thesis examiner)

Jordan Monnink, MA (Psychology), The CSI-effect and the impact of perceived realism (Thesis examiner)

Farshad Daliri, MASc(HCI), Visual Feedback to Perform Bend Gestures on Flexible Displays (Defense chair)

Ravina Samaroo, MA(HCI), Intent-gesture relationships for collaborative information visualization (Thesis examiner)

Laila Goubran, MA(HCI), Information Collection in Forest Fire Response Operations; A Foundation for Situation Awareness (Thesis examiner)

2014 Xiao Du, MASc(HCI), Design and Evaluation of a Learning Assistant System with Optical Head-Mounted Display (OHMD) (Thesis examiner)

Stevenson Gossage, MCS, Understanding the Digital Cardwall for Agile Software Development (Thesis examiner)

2013 Monica Zaczynski ,MASc(HCI), Efficacy Before Novelty: Establishing Design Guidelines in Interactive Gaming for Rehabilitation and Training (Thesis examiner)

Jessica Lo, MASc(HCI) FlexGames: Designing Interactions for Mobile Games with Flexible Devices (Thesis examiner)

**PhD Comprehensive Exam Committees**

| | |
|---|---|
| 2021 | Evan Crothers, University of Ottawa, Topic: Usable Security |
| 2019 | Eric Spero, Carleton University, Topic, HCI |
| 2018 | Christopher Bellman, Carleton University, Topic: HCI<br>Sana Maqsood, Carleton University, Topic: HCI |
| 2017 | Reham Ebada, Carleton University, Topic: Computer Security |
| 2016 | Amal Anda, University of Ottawa, Topic: HCI<br>Mehdi Salehi, University of Ottawa, Topic: Usable Security |
| 2015 | Malak Baslyman, University of Ottawa. Topic: HCI<br>Farah Chanchary, Carleton University. Topic: HCI<br>Ambrose Chow, University of Ottawa. Topic: Computer Security |
| 2014 | Hala Assal, Carleton University. Topic: Computer Security<br>Carsten Grimm, Carleton University. Topic: Usable security<br>Ann Fry, Carleton University. Topic: HCI |
| 2013 | Elizabeth Stobert, Carleton University, Topic: Computer Security |
| 2012 | David Barrera, Carleton University. Defense chair<br>Ahmed Orabi, University of Ottawa. Topic: HCI |

## 7. Teaching

Average overall score out of 5 from teaching evaluations at Carleton University

| | 2011/12 | 2012/13 | 2013/14 | 2014/15 | 2015/16 | 2016/17 | 2018/19 | 2019/20 |
|---|---|---|---|---|---|---|---|---|
| COMP3008 | | | 4.15 | | 4.15 | | | |
| COMP5900/5115 | 4.91 | 4.88 | 4.86 | 4.85 | 4.89 | | 4.80 | 4.77 |
| HCIN5200 | | | | | | 4.81 | | |

Awarded the *2014 Excellence in Graduate Teaching* award by the Graduate Students' Association based on nominations from past graduate students in COMP5900

| | |
|---|---|
| 2021 – 22 | HCIN5100 – Fundamentals of HCI Design and Evaluation (Sept 2021, online)<br>HCIN5900 – Directed Studies (Usable Security & Privacy, students: A. Mann and K. Chaudhry) (January 2022, online) |
| 2020 – 21 | COMP 3008 – Human Computer Interaction (Sept 2020, online)<br>COMP 5110 – Security and Usability (Sept 2020, online) |
| 2019 – 20 | COMP 5110 – Security and Usability (Sept 2019) |
| 2018 – 19 | COMP 5110 – Security and Usability (Sept 2018) |
| 2016 – 17 | HCIN 5200 – Software and User Interface Development (Sept 2016) |
| 2015 – 16 | COMP 3008 – Human Computer Interaction (Jan 2016)<br>COMP 5110 – Security and Usability (Sept 2015) (new course number) |
| 2014 – 15 | COMP 5900 – Security and Usability (Sept 2014) |
| 2013 – 14 | COMP 3008 – Human Computer Interaction (Jan 2014)<br>COMP 5900 – Security and Usability (Sept 2013) |
| 2012 – 13 | COMP 5900 – Security and Usability (Jan 2013) |
| 2011 – 12 | COMP 5900 – Security and Usability (Jan 2012) |
| 2001 – 05 | Teaching 3 or 4 first year computer science classes per year, in-person and online. Managing a large multi-section class with several instructors and TAs. University of Saskatchewan |

**Teaching-related Professional Development**

2022

Equity, Diversity, Inclusion (EDI) concentration of Student Support Certificate

Carleton professional development workshops:

- Safer Spaces Program (CUSSP)
- Accessibility in Higher Education
- Building Student Resilience
- Effective Communication and De-escalation skills
- LivingWorks Start suicide prevention workshop
- NSERC Discovery Grant workshop
- NSERC Equity, Diversity, Inclusion workshop

2020 Carleton Educational Development Centre workshops:

- Preventing Plagiarism through Design
- Introduction to CU Portfolio
- How to design the learning to make the most of this type of delivery and go beyond the simple digitalization of the traditional classroom
- Designing experiential learning activities for the online classroom
- How to engage online learners in authentic assessment

2019 Carleton Student Support Certificate. Completed 15-hour series of workshops on how to more effectively support students (Communication, referrals, indigenous cultural awareness, cross-cultural competence, sexual violence response, supporting students in distress, Safer Spaces LGBT+ support)

2012 Faculty Teaching Certificate, 12 week course, Carleton

2011 Workshop on disabilities, accommodations, and models of inclusive and accessible learning environments, Carleton

2011 Workshop on Asperger's, psychiatric disabilities, learning disabilities, and ADHD, Carleton

2001 Graduate University Teaching Certificate, 1-year course. University of Saskatchewan

# M. Jason Hinek

*Curriculum Vitae*

School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, Ontario, K1S 5B6, Canada

Office: HP 5332
Phone: 613-520-2600 ext 4359
Email: jason.hinek@carleton.ca

## Current position

2023-present *Instructor III and Associate Director (Outreach & Recruitment), Confirmed*
School of Computer Science, Carleton University, Canada

## Previous appointments, promotions and leaves

School of Computer Science, Carleton University, Canada

2023 *Associate Director (Outreach & Recruitment)*
2020 Promotion to *Instructor III*
2019-2020 *Sabbatical Leave (July 2019 – July 2020)*
2018 *Confirmed*
2016 Promotion to *Instructor II*
2017 *Parental Leave (January 2017 – April 2017)*
2014-2015 *Parental Leave (September 2014 – April 2015)*
2012 *Instructor I*

Other Institutions

2011-2012 *Sessional Instructor* (W11, S11, F11, W12, S12)
David R. Cheriton School of Computer Science, University of Waterloo, Canada
2011-2012 *Consultant*
Maplesoft, a subsidiary of Cybernet Systems Co. Ltd, Waterloo, Canada
2010-2011 *Research Associate*
Department of Combinatorics & Optimization, University of Waterloo, Canada
2007-2008 *Postdoctoral Fellow*
Department of Computer Science, University of Calgary, Canada

## Education

2007 PhD in Computer Science, University of Waterloo
2002 MMath in Combinatorics & Optimization, University of Waterloo
2000 BMath in Computer Science and Combinatorics & Optimization, University of Waterloo
1997 MSc in Physics, University of Waterloo
1994 BSc in Physics, University of Windsor

## Professional development

2018- Student Support Cetificate, in progress, Carleton University
- Cross Cultural Competence Training (2018)
- Effective Communication and De-Escalation Skills (2019)
- safeTALK (2019)
- Student Privacy Awareness Training (2019)
- Accessibility in Higher Education (2020)
- Building Student Resilience (2020)
- Indigenous Cultural Awareness Workshop (2020)
- Responding to Disclosures of Sexual Violence (2020)
- Supporting Students in Distress(2020)

2014 Certificate in University Teaching, EDC, Carleton University
2014 Certificate in Blended and Online Teaching, EDC, Carleton University
2012 Instructional Skills Workshop, CTE, University of Waterloo
2011 Teaching Development Seminar Series for Postdoctoral Fellows, CTE, Waterloo

CONFERENCES, WORKSHOPS AND SYMPOSIUMS ATTENDED

2022 *ACM Celebration of Women in Computing (CAN-CWiC)*, Toronto
2019 *Grace Hopper Celebration (GHC 19)*, Orlando, Florida
2019 *ACM Celebration of Women in Computing (CAN-CWiC)*, Mississauga
2017 *ACM Celebration of Women in Computing (CAN-CWiC)*, Montreal
2016 *ACM Celebration of Women in Computing (CAN-CWiC)*, Ottawa
2015 *Welcome to My Classroom: Creating a Positive Learning Environment* workshop,
Educational Development Centre, Carleton University
2015 *Multiple Choice Retreat*,
Educational Development Centre, Carleton University
2012 *Opportunities and New Directions Conference: A Research Conference on Teaching and Learning*,
Centre for Teaching Excellence, University of Waterloo (4th OND Conference)
2011 *Symposium on Teaching Mathematics in Higher Education*,
Math and Statistics Learning Centre, Centre for Teaching and Learning, University of Toronto Scarborough
2011 *Opportunities and New Directions Conference: A Research Conference on Teaching and Learning*,
Centre for Teaching Excellence, University of Waterloo (3rd OND Conference)

## Student supervision

2021 Forest Anderson, PSGL Project (W21)
Project: Creating content for first year courses via Hackathon
2020 Ke Xu, Honours project (F20)
Topic: InterPlanetary Messaging Honours Project
Pravallika Katragunta, PSGL (F20)
Project: First year study group manager
Kevin Sullivan, SaPP (F20)
Project: Created exercise content for COMP1405/1005 Online Textbook
2019 Matthew Auld, Honours project (F19)
Topic: Use of Attribute-Based Encryption in Content-Addressed Distributed Networks

2017 Brandon Marshall, Honours project (F17)
Topic: Security Capture the Flag
2016 Sean Singh, Honours Project (F16)
Topic: Public-Key Cryptography in Wireless Sensor Networks

## Teaching experience

SCHOOL OF COMPUTER SCIENCE, CARLETON UNIVERSITY

| | | |
|---|---|---|
| Summer 2023 | COMP 1005/1405 – Introduction to Computer Science I | (sole instructor; one section) |
| Winter 2023 | COMP 1006 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP 1406 – Introduction to Computer Science I | (instructor for one of three sections) |
| | COMP 3109 – Applied Cryptography & Authentication | (sole instructor; one section) |
| Fall 2022 | COMP 1006 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP 1406 – Introduction to Computer Science I | (sole instructor; one section) |
| Winter 2022 | COMP 1006 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP 1406 – Introduction to Computer Science I | (instructor for one of three sections) |
| | COMP 3109 – Applied Cryptography & Authentication | (sole instructor; one section) |
| Fall 2021 | COMP 1006 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP 1406 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP 2402 – Abstract Data Types and Algorithms | (sole instructor; two sections) |
| | COMP 3109 – Applied Cryptography & Authentication | (sole instructor; one section) |
| Summer 2021 | COMP 1005/1405 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP Matters | (sole instructor) |
| Winter 2021 | COMP 1406 – Introduction to Computer Science II | (instructor for two of three sections) |
| | COMP 1005 – Introduction to Computer Science I | (sole instructor; one section) |
| Fall 2020 | COMP 1405 – Introduction to Computer Science I | (instructor for one of three sections) |
| | COMP 4109 – Applied Cryptography | (sole instructor; one section) |
| Summer 2020 | COMP 1405/1005 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP Matters | (sole instructor) |
| Fall 2019 | COMP 4109 – Applied Cryptography | (sole instructor; one section) |
| Summer 2019 | COMP 1406 – Introduction to Computer Science II | (sole instructor; one section) |
| Winter 2019 | COMP 1406 – Introduction to Computer Science II | (sole instructor; three sections) |
| | COMP 1805 – Discrete Structures I | (instructor for one of three sections) |
| Fall 2018 | COMP 2402 – Abstract Data Types and Algorithms | (sole instructor; two sections) |
| | COMP 4109 – Applied Cryptography | (sole instructor; one section) |
| Summer 2018 | COMP 1406/1006 – Introduction to Computer Science II | (sole instructor; one section) |
| Winter 2018 | COMP 1006 – Introduction to Computer Science II | (sole instructor; one section) |
| | COMP 1406 – Introduction to Computer Science II | (instructor for one of two sections) |
| | COMP 1805 – Discrete Structures I | (instructor for one of two sections) |
| Fall 2017 | COMP 1005 – Introduction to Computer Science I | (instructor for one of two sections) |
| | COMP 1406/1006 – Introduction to Computer Science II | (sole instructor; one section) |
| | COMP 4109 – Applied Cryptography | (sole instructor; one section) |
| Summer 2017 | COMP 1406/1006 – Introduction to Computer Science II | (sole instructor; one section) |
| Fall 2016 | COMP 1005 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP 1406/1006 – Introduction to Computer Science II | (sole instructor; one section) |
| | COMP 4109 – Applied Cryptography | (sole instructor; one section) |

| | | |
|---|---|---|
| Summer 2016 | COMP 1406/1006 – Introduction to Computer Science II | (sole instructor; one section) |
| Winter 2016 | COMP 1406 – Introduction to Computer Science II | (instructor for one of two sections) |
| | COMP 1805 – Discrete Structures I | (instructor for one of two sections) |
| | COMP 2402 – Abstract Data Types and Algorithms | (sole instructor; one section) |
| Fall 2015 | COMP 1805 – Discrete Structures I | (sole instructor; one section) |
| | COMP 2402 – Abstract Data Types and Algorithms | (instructor for one of two sections) |
| | COMP 4109 – Applied Cryptography | (sole instructor; one section) |
| Summer 2015 | COMP 1405/1005 – Introduction to Computer Science I | (sole instructor; one section) |
| Summer 2014 | COMP 1406/1006 – Introduction to Computer Science II | (sole instructor; one section) |
| Winter 2014 | COMP 1805 – Discrete Structures | (sole instructor; one section) |
| | COMP 3804 – Design and Analysis of Algorithms I | (sole instructor; one section) |
| | COMP 1406 – Introduction to Computer Science II | (tutorial creation) |
| Fall 2013 | COMP 1406/1006 – Introduction to Computer Science II | (sole instructor; one section) |
| | COMP 1805 – Discrete Structures | (sole instructor; one section) |
| | COMP 4109 – Applied Cryptography | (sole instructor; one section) |
| Summer 2013 | COMP 1406/1006 – Introduction to Computer Science II | (sole instructor; one section) |
| Winter 2013 | COMP 1006 – Introduction to Computer Science II | (sole instructor; one section) |
| | COMP 1405/1005 – Introduction to Computer Science I | (sole instructor; one section) |
| | COMP 2001/2401 – Introduction to Systems Programming | (sole instructor; one section) |
| Fall 2012 | COMP 1405 – Introduction to Computer Science I | (tutorial instructor; three sections) |
| | COMP 2401 – Introduction to Systems Programming | (tutorial instructor; three sections) |

Spring 2023 Enrichment Mini Course Program EMCP 2023 – Teach your Computer to Paint
Spring 2022 Enrichment Mini Course Program EMCP 2022 – Teach your Computer to Paint
Spring 2019 Enrichment Mini Course Program EMCP 2019 – Teach your Computer to Paint
Spring 2018 Enrichment Mini Course Program EMCP 2018 – Teach your Computer to Paint
Spring 2017 Enrichment Mini Course Program EMCP 2017 – Teach your Computer to Paint
Spring 2016 Enrichment Mini Course Program EMCP 2016 – Teach your Computer to Paint
Spring 2015 Enrichment Mini Course Program EMCP 2015 – Teach your Computer to Paint

DAVID R. CHERITON SCHOOL OF COMPUTER SCIENCE, UNIVERSITY OF WATERLOO

| | | |
|---|---|---|
| Spring 2012 | CS 246 – Object-Oriented Software Development | (sole instructor; two sections) |
| Winter 2012 | CS 136 – Elementary Algorithm Design and Data Abstraction | (instructor for one of six sections) |
| | CS 240 – Data Structures and Data Management | (instructor for one of two sections) |
| Fall 2011 | CS 241 – Foundations of Sequential Programs | (instructor for one of three sections) |
| | CS 341 – Algorithms | (instructor for one of three sections) |
| Spring 2011 | CS 116 – Introduction to Computer Science 2 | (sole instructor; two sections) |
| Winter 2011 | CS 116 – Introduction to Computer Science 2 | (instructor for two of nine sections) |
| Winter 2007 | CS 126DE – Introduction to Software Development | (sole instructor; distance education course) |
| Winter 2006 | CS 134 – Principles of Computer Science | (instructor for one of nine sections) |

PRIVATE TUTOR

2000-2004 Office for Persons with Disabilities, University of Waterloo
Computer science, mathematics and physics

## Academic and community service

### CARLETON UNIVERSITY

2021 Canada Wide Science Fair (outreach presentation)
2020-present EDI Committee in SCS
2015-present Women in Compute Science (WiCS) group
2015-present SCS Teaching Group
2013-present Co-op work term report grading

2023 EMCP 2023 instructor – *Teach your computer to paint*
2022 EMCP 2022 instructor – *Teach your computer to paint*
2019 EMCP 2019 instructor – *Teach your computer to paint*
2018 EMCP 2018 instructor – *Teach your computer to paint*
2017 EMCP 2017 instructor – *Teach your computer to paint*
2016 EMCP 2016 instructor – *Teach your computer to paint*
2015 EMCP 2015 instructor – *Teach your computer to paint*

2015 Speaker at "what I wish I knew in first/second year" seminars hosted by CCSS
2013 Speaker at "what I wish I knew in first year" seminar hosted by CCSS

2016 Chair of the Honour's Project Committee
2015 Honour's Project Demo Day, Organizer
2012-2014 Member of the Curriculum Committee
2013-2014 Member of the Promotion/Tenure Committee

### PREVIOUS SERVICE

2011 *Oral presentation judge*
Graduate Student Research Conference 2011, University of Waterloo
2007-2008 *Security representative*
Laptop Encryption Group, University of Calgary
2007-2008 *Organizer*
iCORE Information Security Lab Security Seminars, University of Calgary
2005-2007 *Co-founder and co-organizer*
St. Paul's Graduate Apartments Residents' Association, University of Waterloo
2004-2007 *Principal organizer*
Centre for Applied Cryptographic Research Seminar Series, University of Waterloo
2005-2006 *Graduate student representative*
School Advisory Committee on Appointments (SACA), David R. Cheriton School of Computer Science, University of Waterloo
2001-2006 *Organizer* (2004, 2005, 2006), *cast member* (2001, 2003) "The Math Faculty Players"
Math Faculty Graduate Student Teaching Assistant Orientation Seminar, University of Waterloo
2003 *Graduate student representative*
Computer Science Computing Facility (CSCF) Advisory Committee, School of Computer Science, University of Waterloo
1993-1994 *Co-founder and vice-president*
Physics Club, University of Windsor

EXTERNAL REVIEWER FOR JOURNALS

2002-present Advances in Mathematics of Communications, Computers and Mathematics with Applications, Designs, Codes and Cryptography, IEEE Transactions on Information Theory, Information Processing Letters, Information and Computation, Journal of Computer Science and Technology, Journal of Symbolic Computation, Journal of Systems and Software, Security and Communication Networks, Theoretical Computer Science

EXTERNAL REVIEWER FOR PEER-REVIEWED CONFERENCES

2003-present Progress in Cryptology - AFRICACRYPT 2012
Selected Areas in Cryptography - SAC 2011
Australasian Conference on Information Security and Privacy - ACISP 2006, 2011, 2013
Advances in Cryptology - ASIACRYPT 2005, 2006
Advances in Cryptology - CRYPTO 2006
Advances in Cryptology - EUROCRYPT 2004, 2005, 2008, 2013
Conference on Computer and Communications Security - ASIACCS 2008
The Cryptographer's Track at RSA Conference - CT-RSA 2008, 2010
Information Security and Privacy - ACISP 2006
Public Key Cryptography - PKC 2005, 2006, 2007
Security in Communication Networks - SCN 2004

## Education detail

2007 Doctor of Philosophy (Ph.D.), Computer Science (CS) GPA: 92.5%
University of Waterloo, Waterloo, Ontario, Canada
Thesis: *On the Security of Some Variants of RSA*
Advisers: Mark Giesbrecht and Doug Stinson

2002 Master of Mathematics (M.Math), Combinatorics & Optimization (C&O) GPA: 92.0%
University of Waterloo, Waterloo, Ontario, Canada
Thesis: *Low Public Exponent Partial Key and Low Private Exponent Attacks on Multi-prime RSA*
Adviser: Edlyn Teske

2000 Bachelor of Mathematics (B.Math), Joint CS and C&O GPA: 91.3%
University of Waterloo, Waterloo, Ontario, Canada
With Distinction – Dean's Honour List

1997 Master of Science (M.Sc.), Physics GPA: 84.8%
University of Waterloo, Waterloo, Ontario, Canada
Thesis: *2D Time Domain NMR Study of Wood*
Adviser: Hartwig Peemoeller

1994 Bachelor of Science (B.Sc.), Honours Physics GPA: 12.5/13 (major)
University of Windsor, Windsor, Ontario, Canada 12/13 (cumulative)
Awarded Board of Governors Medal (for top graduating Physics student)
College Bowl team member, 1991-1992 season

CONTINUED EDUCATION

2014 Certificate in University Teaching, Certificate
Educational Development Centre, Carleton University, Ottawa, Ontario, Canada
Description: The goal of the program is to provide participants with a safe and supportive environment to enhance their appreciation of sound pedagogy, strengthen their teaching skills and explore new approaches to instruction. Together these three areas will contribute to helping you become more efficient, effective and confident in enhancing the learning environment for your students.

2014 Certificate in Blended and Online Teaching, Certificate
Educational Development Centre, Carleton University, Ottawa, Ontario, Canada
Description: Participants will develop a manageable plan for designing an online course, create an online module for an upcoming course, learn to engage and motivate students in online learning environments and evaluate available educational technologies in relation to learning outcomes.

2012 Instructional Skills Workshop, Certificate
Centre for Teaching Excellence, University of Waterloo, Waterloo, Ontario, Canada
Description: The Instructional Skills Workshop is a 24-hour series of microteaching sessions with peer feedback. It leads to a widely-recognized Certificate and includes instruction in learning theories as well as considerable application and practice.

2011 Teaching Development Seminar Series for Postdoctoral Fellows, Certificate
Centre for Teaching Excellence, University of Waterloo, Waterloo, Ontario, Canada
Description (excerpt): The program consists of six seminars, as well as optional activities such as individual work and course design consultations. The seminars provide interactive and hands-on experience for participants and employ a variety of teaching and learning activities, such as group work, videos, and discussions.

## Honours & awards

2012 Top Instructor Recognition for CS 241 (Fall 2011 Semester)
David R. Cheriton School of Computer Science, University of Waterloo
2001 Nominated for the Outstanding Teaching Assistant Award
Department of Combinatorics & Optimization, University of Waterloo
2000 Graduated with distinction – Dean's Honour List
BMath, University of Waterloo
1999 Outstanding Teaching Assistant Award (Graduate Student)
Department of Physics, University of Waterloo
1994 Board of Governors Medal for Physics
University of Windsor
1992 Hewlett-Packard Calculator Award
University of Windsor

SCHOLARSHIPS HELD AT THE UNIVERSITY OF WATERLOO

2006 Doctoral Thesis Completion Award
2002-2004 GO-Bell Scholarship

2000-2002 Ontario Graduate Scholarship
1998-2000 University of Waterloo Senate Scholarship
1994-1996 NSERC–PGSA
1994-1995 Graduate Entrance Scholarship
1994-1995 Physics Department Entrance Scholarship

SCHOLARSHIPS HELD AT THE UNIVERSITY OF WINDSOR

1992-1994 NSERC Undergraduate Summer Research Award (1992, 1993, 1994)
1992-1994 Nicolaus Copernicus Scholarship (1992, 1993, 1994)
1990-1994 Canada Scholarship
1990-1994 John B. Kennedy Scholarship
1990-1994 University of Windsor Entrance Scholarship
1990-1991 Local 444 Retirees Scholarship

## Publications

BOOKS

2009 M. Jason Hinek, *Cryptanalysis of RSA and Its Variants*, Chapman & Hall/CRC, Boca Raton, 2009, 272 pp.

JOURNAL ARTICLES

2013 H. Peemoeller, W.P. Weglarz, M. J. Hinek, R. Holly, C. Lemaire, R. Teymoori, J. Liang, J. Crone, F. K. Mansour and I. D. Hartley, NMR detection of liquid-like wood polymer component in dry aspen wood , *Polymer*, 54(5): 1524-1529, February 2013.

2012 M. Jason Hinek, Shaoquan Jiang, Rei Safavi-Naini and Siamak Shahandashti, Attribute-Based Encryption without Key Cloning, *International Journal of Applied Cryptography*, 2(3): 250–270, 2012.

2010 M. Jason Hinek and Charles Lam, Common Modulus Attacks on Small Private Exponent RSA and Some Fast Variants (in Practice), *Journal of Mathematical Cryptology*, 4(1): 58–93, July 2010.

2009 Hung-Min Sun, Mu-En Wu, M. Jason Hinek, Cheng-Ta Yang and Vincent S. Tseng, Trading Decryption for Speeding Encryption in Rebalanced-RSA, *Journal of Systems and Software*, 82(9): 1503–1512, September 2009.

2009 M. Jason Hinek and Charles Lam, Another Look at Some Fast Modular Arithmetic Methods, *Journal of Mathematical Cryptology*, 3(2):165–174, August 2009.

2008 M. Jason Hinek, On the Security of Multi-prime RSA, *Journal of Mathematical Cryptology*, 2(2):117–147, July 2008.

2007 Hung-Min Sun, Mu-En Wu, Wei-Chi Ting and M. Jason Hinek, Dual RSA and Its Security Analysis, *IEEE Transactions on Information Theory*, 53(8):2922–2933, August 2007.

1994 W. Kedzierski, J. Supronowicz, A. Czajkowski, M. J. Hinek, J. B. Atkinson and L. Krause, The Rotationally Resolved $G0_u^+ \leftarrow A0_g^+$ Electronic Spectrum of the $(^{202}Hg)_2$ Excimer, *Chemical Physics Letters*, 218(4):314–319, February 1994.

1993 J. Supronowicz, M. J. Hinek, J. B. Atkinson and L. Krause, Mixing of the Cd $5^3$ P Fine-Structure States by Hg Collisions, *Chemical Physics Letters*, 213(3-4):282–288, October 1993.

REFEREED CONFERENCE PAPERS

2006 M. Jason Hinek, Another Look at Small RSA Exponents, *Lecture Notes in Computer Science*, 3860:82–86, 2006 (CT-RSA 2006).

2002 M. J. Hinek, Mo King Low and Edlyn Teske, On some Attacks on Multi-prime RSA,*Lecture Notes in Computer Science*, 2595:385–404, 2003 (SAC 2002).

THESES

2007 On the Security of RSA and Its Variants, Ph.D. Thesis, David R. Cheriton School of Computer Science, University of Waterloo, 2007.

2002 Low Public Exponent Partial Key and Low Private Exponent Attacks on Multi-prime RSA. Masters Thesis, Department of Combinatorics & Optimization, University of Waterloo, 2002.

1997 2D Time Domain NMR Study of Wood. Masters Thesis, Department of Physics, University of Waterloo, 1997.

TECHNICAL REPORTS

2009 M. Jason Hinek and Charles Lam, Common Modulus Attacks on Small Private Exponent RSA and Some Fast Variants (in Practice), Cryptology ePrint Archive: Report 2009/037, 2009.

2008 M. Jason Hinek, Shaoquan Jiang, Rei Safavi-Naini and Siamak Shahandashti, Attribute-Based Encryption with Key Cloning Protection, Cryptology ePrint Archive: Report 2008/487, 2008.

2006 M. Jason Hinek, On the Security of Multi-prime RSA, Technical Report CACR 2006-16, University of Waterloo, 2006.

2006 M. Jason Hinek and Douglas R. Stinson, An Inequality about Factors of Multivariate Polynomials,Technical Report CACR 2006-15, University of Waterloo, 2006.

2005 Hung-Min Sun, M. Jason Hinek and Mu-En Wu, On the Design of Rebalanced RSA-CRT, Technical Report CACR 2005-35, University of Waterloo, 2005.

2005 M. Jason Hinek, Small Private Exponent Partial Key-Exposure Attacks on Multiprime RSA, Technical Report CACR 2005-16, University of Waterloo, 2005.

2004 M. Jason Hinek, Lattice Attacks in Cryptography: A Partial Overview , Technical Report CACR 2004-08, University of Waterloo, 2004.

2004 M. Jason Hinek, New Partial Key Exposure Attacks on RSA Revisited, Technical Report CACR 2004-02, University of Waterloo, 2004.

2004 M. Jason Hinek, (Very) Large RSA Private Exponent Vulnerabilities, Technical Report CACR 2004-01, University of Waterloo, 2004.

2002 M. Jason Hinek, On Some Attacks on Multi-Prime RSA, Technical Report CORR 2002-11, University of Waterloo, 2002.

## Seminars and conference talks

2009 Towards Attribute-Based Encryption Without Key Delegation
CACR Cryptography Seminar, University of Waterloo. October 1, 2009.

2008 Lattice Basis Reduction – A Fine Cryptanalytic Tool
iCIS Security Seminar, University of Calgary. January 25, 2008.

2007 Some Nice Applications of Lattice Basis Reduction
CACR Cryptography Seminar, University of Waterloo. March 21, 2007.

2006 Another Look at Small RSA Exponents
CT-RSA 2006, McEnery Convention Center, San Jose, Ca. February 14, 2006.

2005 Cryptanalysis of 'More Short' RSA Secret Exponents
CACR Cryptography Seminar, University of Waterloo. July 7, 2005.

2004 On the equivalence of computing the RSA secret key and factoring
CACR Cryptography Seminar, University of Waterloo. October 21, 2004.

2004 Some dangers of third party RSA key generation
CACR Cryptography Seminar, University of Waterloo. March 8, 2004.

2002 Small Vectors in Lattices : Some Useful Applications
Applied Math Graduate Seminar Series, University of Waterloo. November 15, 2002.

2002 On Some Attacks on Multi-prime RSA
SAC 2002, Memorial University, St. John's, Newfoundland. August 16, 2002.

2002 A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding
CACR Cryptography Seminar, University of Waterloo. April 8, 2002.

# Christine Laurendeau


| | | | |
|---|---|---|---|
| Address: | School of Computer Science<br>Carleton University<br>1125 Colonel By Drive<br>Ottawa, ON K1S 5B6 | Office:<br>Phone:<br>E-mail:<br>Web: | 5320 HP<br>613-520-2600 ext.1253<br>christine.laurendeau@carleton.ca<br>carleton.ca/scs/people/christine-laurendeau/ |


## Education

09/2005 – 05/2009: **Ph.D. Computer Science**, Carleton University

09/1989 – 09/1992: **M. Computer Science**, University of Ottawa

09/1984 – 12/1988: **B.Sc. Computer Science** (Cooperative Education Program), University of Ottawa
Honours: *Summa cum laude*

## Professional Development

12/2021: Kinàmàgawin Indigenous Learning Certificate, Carleton University

09/2021: "Indigenous Canada" (12-week MOOC course), University of Alberta

06/2011: Certificate in University Teaching, Educational Development Centre, Carleton University

## Achievement Awards

| Year | Award |
|---|---|
| 2020 | Nominee for Carleton University residence students' Favourite Faculty Member |
| 2013 | Nominee for Capital Educators' Award |
| 2012 | Nominee and Carleton University Finalist for Capital Educators' Award |
| 2007 – 2009 | NSERC Canada Graduate Scholarship (CGS-D2) |
| 2007 – 2009 | Carleton University Academic Achievement Award |
| 1992 | Master's thesis nominated for a prize (Governor General's Gold Medal, Senate Medal) |
| 1989 – 1991 | NSERC Post-Graduate Scholarship (PGM) |
| 1989 – 1991 | University of Ottawa Graduate Scholarship |
| 1989 | Ontario Graduate Scholarship (declined) |
| 1989 | Prize for the highest standing in Computer Science, University of Ottawa |
| 1986 – 1988 | Dean's Honour List, University of Ottawa |
| 1984 | University of Ottawa Scholarship for Academic Excellence |

## Skills

| | |
|---|---|
| Teaching expertise: | Software engineering; systems programming; programming languages (C/C++, Java); wireless networks and security |
| Methodologies: | Object-oriented analysis and design; Knowledge engineering; GUI design |
| Programming Languages: | C/C++; Java; Prolog |
| Business Management: | Board of directors leadership; Technical team leadership; Training and mentoring |
| Natural Languages: | Perfectly bilingual (French and English) in script and speech |

## Work Experience

### ➢ Academic

| Period | Position | University | Mandate |
|---|---|---|---|
| 07/2009 – present | Instructor | Carleton University | Teaching at the undergraduate level |
| 09/2005 – 06/2009 | Research Assistant | Carleton University | Research in wireless communications security |
| 09/1989 – 09/1992 | Research Assistant | University of Ottawa | Research in natural language processing |

### ➢ Teaching University Courses (Carleton University)

| Course | Title | Semesters |
|---|---|---|
| COMP 2404 | "Introduction to Software Engineering" (formerly “Programming in C++”) | W23, W21, F20, W20, W19, F18, W17, F16, W16, F15, W15, F14, W14, W13, W12, W11, W10, F09 |
| COMP 2401 | “Introduction to Systems Programming” | F22, F21, F20, F18, F16, W16, F15, F14, F13, F12, F11, F10 |
| COMP 3004 | “Object-Oriented Software Engineering” | F19, W19, W17, F15, F14, F13, F12, F11, W11, F10 |
| COMP 4203 | "Wireless Networks and Security" | W20, W18, W12 |
| COMP 1805 | “Discrete Structures I” | W10 |
| COMP 1006 | “Design & Implementation of Computer Applications” | W10 |
| COMP 1005 | “Introduction to Object-Oriented Programming” | W15, F10, F09 |

### ➢ Teaching Mini-Courses (Carleton University)

| Date | Course | Title | Venue | Topic |
|---|---|---|---|---|
| 2008 | EMCP 203 | “Worlds of Imagination: A Window into the Science of Computer Gaming” | Enrichment mini-course | Computer game development |
| 2007<br>2006 | EMCP 203 | “From Magic Waves to Thinking Cars: The Wizardry of Wireless Technology” | Enrichment mini-course | Wireless networks and security |

### ➢ Industry

| Period | Position | Employer | Mandate |
|---|---|---|---|
| 1994 – 1997 | Member of Scientific Staff | Nortel Networks | Software and GUI development |
| 1992 – 1994 | Associate Systems Engineer | SHL Systemhouse | Network interface research |
| 1991 – 1992 | Computer Systems Specialist | Bell Canada | Expert systems research |
| 1989 | Manager – Planning Tools | Bell Canada | Software development |
| 1986 – 1988 | Coop Student | Bell Canada, BNR, MetLife | Software development |

### ➢ Volunteer

| Period | Position | Organization |
|---|---|---|
| 2007 | Webmaster | Sixth International Conference on Ad-Hoc Networks & Wireless |
| 2006 | Conference volunteer | Fifth International Conference on Ad-Hoc Networks & Wireless |
| 2003 – 2004 | President and CEO | Richmond Cooperative Nursery School |
| 2002 – 2003 | Vice-President | Richmond Cooperative Nursery School |

## Administrative Duties at Carleton University and the School of Computer Science (SCS)

### ➢ SCS Deputy Director (2023 - present)

| Duties |
|---|
| • Lead the accreditation process and prepare quality assurance documents |
| • Assist SCS Director with various tasks, including teaching assignments and budget |

### ➢ SCS Associate Director – Recruitment and Outreach (2018 - 2023)

| Duties |
|---|
| • Meet with potential students and their parents |
| • Attend and present at recruitment events |
| • SCS liaison to university recruitment officers |

### ➢ SCS Co-op Coordinator (2014 - 2018)

| Duties |
|---|
| • Faculty advisor to students enrolled in the undergraduate and graduate co-op programs |
| • Coordinating grading of work term reports |

### ➢ SCS Associate Director – Undergraduate (2011 - 2014)

| Duties |
|---|
| • Faculty advisor to undergraduate students |
| • Creation and management of Computer Science Tutorial Assistance Centre |
| • Management of teaching assistants, including assignation to courses |
| • Selection of departmental award recipients |
| • Liaison to undergrad student society (Carleton Computer Science Society) |

### ➢ Committee memberships

| Period | Duty |
|---|---|
| 07/2023 – present | Chair, SCS Curriculum committee |
| 07/2023 – present | Member, Faculty of Science SCAP committee |
| 01/2021 – present | Member, SCS Instructor Hiring committee |
| 09/2019 – present | Member, Faculty of Science Admissions committee |
| 07/2020 – 06/2023 | Member, Carleton University Senate |
| 09/2020 – 06/2023 | Member, SCS Curriculum committee |
| 01/2019 – 04/2021 | CUASA Member, Joint Parity Committee on Instructors |
| 09/2021 – 12/2021 | External member, CSIT Instructor Hiring committee |
| 10/2019 – 05/2020 | External member, SCE Assoc. Professor and Instructor Hiring committee |
| 10/2019 – 04/2020 | Member, SCS Instructor Hiring committee |
| 01/2019 – 05/2019 | Member, SCS Instructor Hiring committee |
| 08/2015 – 06/2017 | Founder and member, SCS Teaching Group |
| 10/2014 – 06/2017 | Member, Carleton Teaching and Learning Council |
| 08/2012 – 06/2017 | Member, Carleton Senate Honorary Degrees committee |
| 08/2012 – 06/2015 | Member, Carleton Senate Library committee |
| 08/2011 – 08/2014 | Member, Faculty of Science Recruitment and Retention committee |
| 01/2011 – 06/2014 | Member, SCS Curriculum Reinvention committee |
| 07/2009 – 06/2011 | Member, SCS Undergraduate Recruitment committee |

## Reviews (research articles and proposals)

| Date | Venue |
|---|---|
| 2014 | IEEE Communications Surveys and Tutorials |
| 2012 | IEEE Journal on Selected Areas in Communications - 2012 Special Issue on Emerging Technologies in Communications |
| 2011 | Ninth Annual Conference on Privacy, Security and Trust (PST 2011) |
| 2009 | Fonds de recherche sur la nature et les technologies, Gouvernement du Québec |
| 2009 | EURASIP Journal on Wireless Communications and Networking |
| 2008 | Journal of Networks |
| 2008 | 3rd ACM Symposium on Information, Computer and Communications Security (ASIACCS 2008) |
| 2006 | Fifth International Conference on Ad-Hoc Networks & Wireless (ADHOC-NOW 2006) |
| 2006 | Second IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2006) |

## Student Supervision

| Year | Name | Course | Topic |
|---|---|---|---|
| 2020 | Adam Hackett | Honours project | Quick-Cart: A Self-Organizing Grocery List Application |
| 2019 | Ebunoluwa Segun | Honours project | EasyCash: A Cash On-Demand Service |
| 2018 | Matthieu Drouin | Honours project | Anonymous and Secure Communication via Bluetooth on Android |
| 2015 | John Cooper | Honours project | Simulation Tool for Evaluating the Station-to-Station Key Agreement Protocol for Data Broadcasting in Mobile Ad Hoc Networks |
| 2015 | Kurt Engsig | Honours project | Secure Peer to Peer Instant Messenger |
| 2015 | Ado Chaddad | Honours project | WhatsInsideThere Framework |
| 2013 | Tom Goldsmith | Honours project | Using Statistical Analysis to Predict the Result of User Interactions With Visual Content |
| 2013 | David Krutsko | Honours project | Navigator: A scriptable software system for automating World of Warcraft |
| 2013 | Carly Hashem & John Byford | Honours project | The Electronic Healthcare Management System |
| 2012 | Bart Wernik | Honours project | ARP Spoof Attack Mitigation and Threat Analysis in Mobile Ad Hoc Networks |
| 2012 | Dean Pearce | Honours project | Augmented Reality Using Geolocation Data and Dynamic Caching |
| 2012 | Austin Chamney | Honours project | Scalability of Broadcast Messages in DSRC Vehicular Networks |
| 2011 | Logan Towers | Independent Study | Cloud Computing |
| 2010 | Jana Sivarajah | Independent Study | A Study of 3GPP Long Term Evolution Technology |
| 2010 | Doug Sceviour | Honours project | Vehicular Velocity Pattern Matching in Intelligent Traffic Systems |
| 2009-2010 | Payal Bhatia | Master's (co-supervised) | Solution to The Wireless Evil-Twin Transmitter Attack |
| 2008 | Scott Broschell | Honours project (co-supervised) | Hyperbolic location estimation for mobile rogue attackers |
| 2007 | Marufur Rahman | Honours project (co-supervised) | Path loss parameters in Wi-Fi networks |
| 2007 | Kevin Nelson | Directed study (co-supervised) | Simulation of signal strength based hyperbolic localization to achieve rogue attribution |
| 2007 | Kevin Nelson | Honours project (co-supervised) | Detection of anomalous position reports |

## Publications

- Refereed Journals
  - C. Laurendeau and M. Barbeau, "Centroid Localization of Uncooperative Nodes in Wireless Networks Using a Relative Span Weighting Method," *EURASIP Journal on Wireless Communications and Networking,* Volume 2010, 10 pages, January 2010.
  - C. Laurendeau and M. Barbeau, "Probabilistic Localization and Tracking of Malicious Insiders Using Hyperbolic Position Bounding in Vehicular Networks," *EURASIP Journal on Wireless Communications and Networking, Special issue on Wireless Network Security,* Volume 2009, 13 pages, July 2009.
  - C. Laurendeau and M. Barbeau, "Probabilistic Evidence Aggregation for Malicious Node Position Bounding in Wireless Networks," *Journal of Networks,* 4(1): 9:18, February 2009.
  - C. Laurendeau and M. Barbeau, "Insider Attack Attribution Using Signal Strength Based Hyperbolic Location Estimation," *Security and Communication Networks,* Wiley InterScience, 1(4): 337-349, July-August 2008.
- Refereed Conferences
  - P. Bhatia, M. Barbeau and C. Laurendeau, "Solution to the Wireless Evil-Twin Transmitter Attack," *Proceedings of the 5th International Conference on Risks and Security of Internet and Systems,* October 2010.
  - C. Laurendeau and M. Barbeau, “Relative Span Weighted Localization of Uncooperative Nodes in Wireless Networks," *Proceedings of the International Conference on Wireless Algorithms, Systems and Applications (WASA),* August 2009.
  - C. Laurendeau and M. Barbeau, "Hyperbolic Location Estimation of Malicious Nodes in Mobile WiFi/802.11 Networks," in *Proceedings of the 2nd IEEE LCN Workshop on User MObility and VEhicular Networks (ON-MOVE)*, October 2008.
  - C. Laurendeau and M. Barbeau, "Secure Anonymous Broadcasting in Vehicular Networks," in *Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN),* pages 661-668, October 2007.
  - C. Laurendeau and M. Barbeau, "Threats to Security in DSRC/WAVE," in *Ad-Hoc, Mobile, and Wireless Networks: Proceedings of the 5th International Conference (ADHOC-NOW),* volume 4104 of Lecture Notes in Computer Science, pages 266-279, Springer Berlin/Heidelberg, 2006.
- Theses
  - C. Laurendeau, "Location Tracking Mitigation For Honest Nodes and Location Estimation of Uncooperative Devices in Wireless Mobile Networks," *Ph.D. Thesis*, Carleton University, 2009.
  - C. Laurendeau, "Automated Acquisition of Technical Concepts From Unrestricted English Text Using Noun Phrase Classification," *Master's Thesis*, University of Ottawa, 1992.
- Book Chapter
  - M. Barbeau and C. Laurendeau, "Analysis of Threats to WiMAX/802.16 Security," in Y. Zhang and H.-H. Chen, editors, *Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Networks*, chapter 15, pages 347-362, Auerbach Publications, 2008.
- Feature Article
  - M. Barbeau and C. Laurendeau, "Tilting at Giants: Avoiding Quixotic Pursuits in Understanding the Threats to Wireless Network Security," in *Connections*, MITACS e-newsletter, September 2007.

## Invited Presentations

- with M. Barbeau, "Malicious Wireless Node Detection Using RSS-based Position Bounding," *MITACS/MASCOS Joint Workshop on Fusion, Mining and Security for Networks,* McGill University, Invited Presentation, June 2008.
- with M. Barbeau and J. García-Alfaro, "Threat Analysis Paradigms in Wireless Technology," *1st Canada-France MITACS Workshop on Foundations & Practice of Security,* Industrial Tutorial, May 2008.
- "Hyperbolic Position Bounding of Malicious Nodes in Wireless Networks," *1st Canada-France MITACS Workshop on Foundations & Practice of Security,* Contributed Talk, May 2008.
- with M. Barbeau, "WiMAX/802.16 Broadband Wireless Networks," *SYTACom Research Workshop,* Concordia University, Invited Presentation, May 2008.
- "Hyperbolic Position Bounding of Malicious Nodes in Wireless Networks," *Carleton-MITACS Wireless Security Day,* Carleton University, Invited Presentation, April 2008.
- "Secure Anonymous Broadcasting in Vehicular Networks," *Carleton Wireless Security Day,* Carleton University, Invited Presentation, March 2007.
- with M. Barbeau, "Threat Analysis in Securing Ad Hoc Networks," *Communication and Security in Ad Hoc Networks, 7th MITACS Annual Conference,* MITACS NCE, Invited Presentation, June 2006.

# Elizabeth Stobert

## Curriculum Vitae

---

### Personal Details

School of Computer Science, Carleton University
1125 Colonel By Drive Ottawa, ON, Canada, K1S 5B6
Email: elizabeth.stobert@carleton.ca

---

### Research Experience

**2019 – Present** **Assistant Professor, School of Computer Science**
**Co-Director, HCI Masters Program**
Carleton University
(On parental leave; August 2021 - June 2022)

**2019** **Associate Research Officer, Digital Technologies Research Centre**
National Research Council of Canada
**Adjunct Research Professor, School of Computer Science**
Carleton University

**2018** **Postdoctoral researcher, Concordia Institute for Information Systems Engineering**
Concordia University
(On parental leave; January - August 2018)

**2015–2017** **Senior researcher, System Security Group**
ETH Zürich

**2011–2015** ***Ph.D.* Computer Science, Carleton University**

**2009–2011** ***M.A.* Cognitive Psychology, Carleton University** (Concentration in HCI)

**2008–2009** ***B.A. Honours*, Psychology, Carleton University**

**2004–2008** ***B.Math.*, Mathematics, Carleton University**

---

### Teaching Experience

**2019–Present** **Assistant Professor (School of Computer Science, Carleton University)**

- COMP 5210: HCI Models, Theories & Frameworks
- HCIN 5100: Fundamentals of HCI Design & Evaluation
- COMP 3301: Technical Writing for Computer Science
- COMP 3008: Human-Computer Interaction

**2017–2018** **Contract Instructor (HCI Masters Program, Carleton University)**

- HCIN 5100: Fundamentals of HCI Design & Evaluation

**2017** **SecHuman Summer School**

**2015–2016** **Co-instructor of Graduate Seminar Course on Current Topics in Information Security (Department of Computer Science, ETH Zürich)**

---

## Student Supervision

**PhD Students**

Aniqa Binte Alam (Co-supervised with Robert Biddle, "Cultural Dimensions of Usable Security", expected graduation 2026)

**Masters Students**

Paola Marmorato (expected graduation 2024)
Ruchi Swami (expected graduation 2024)
Svetlana Dobrynina (Co-supervised with Sonia Chiasson, "Mental Models of Password Managers", graduated 2023)
Joy Smith (Co-supervised with Leah Zhang-Kennedy, "Usable Security Education", graduated 2022)
Aniqa Binte Alam ("Cultural Factors in Password Sharing: A Case Study of Bangladesh", graduated 2021)
Lin Kyi (Co-supervised with Robert Biddle, "End User Mental Models of Social Engineering Attacks", graduated 2021)
Tina Safaie (Student at Concordia University, co-supervised with Mohammad Mannan and Amr Youssef, "ByPass: Easing Password Manager Adoption", graduated 2021)

**Honours Projects**

Clarissa Dayle Fernandez ("Posthumous Password Management", Summer 2022)
Adam Khachi ("Evaluating Security Advice in Infographics", Summer 2022)
Silver Lewis ("Loci PassTiles", Winter 2021)
Guillaume St-Pierre ("Improving Software Documentation Quality and Security Using Automated Documentation Tools", Winter 2021)
Jake Bauer ("Improving the Memorability of Pronounceable Passwords Through Phonological Similarity", Winter 2021)
Sarah Oloumi ("PortioPass: A Password Sharing Application", Fall 2020)
Samuel Mitchell ("A Usability Analysis of Canadian Open Government Data Presentation", Winter 2020)

**Undergraduate Students**

Mary-Emma Barnhill (I-CUREUS, Winter 2023)
Kalumbu Kasaji (DSRI, Summer 2022; I-CUREUS, Summer 2023)
Meera Balsara (DSRI, Summer 2020)

## Funding & Awards

**2023-2025** NRC Aging in Place Challenge Program "Usable Security for Aging in Place" ($141,900)

**2021–2026** SSHRC Partnership Grant "Human-Centric Cybersecurity"

- "Mental Models of Container Security" ($10,000)

**2020** SERENE-RISC Workshop Best Poster "Etics and Emics of Usable Security: Culturally Universal or Culturally Specific?"

**2020–2025** NSERC Discovery Grant "Cognition-Informed Security" ($24,000/year)

**2020–2021** NSERC Discovery Grant Launch Supplement ($12,500)

**2018–2019** NSERC PDF Fellowship ($45,000/year)

**2017–2022** MIWF Förderlinie "Digitale Sicherheit" (€600,000, approx. $900,000) – Declined (Funding awarded from the Ministry of Innovation, Science and Research (MIWF) of the state of North Rhine Westphalia (Germany) for the formation of a research group.)

**2015** Best Paper Award: International Conference on Passwords

**2011–2014** NSERC CGS-D3 Scholarship ($35,000/year)

**2013** Pass with Distinction on PhD comprehensive exams

**2010–2011** NSERC CGS-M Scholarship ($17,500/year)

**2010** $3^{rd}$ place undergraduate finalist in CHI Student Research Competition

**2009–2015** Carleton University Departmental Graduate Scholarships ($5,000/year)

## Service

**Technical Program Committees:**

**2023** USENIX Security Symposium, Symposium on Usable Privacy and Security (SOUPS), New Security Paradigms Workshop (NSPW), ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)

**2022** New Security Paradigms Workshop (NSPW)

**2021** IEEE European Symposium on Security and Privacy (EuroS&P), Symposium on Usable Privacy and Security (SOUPS), New Security Paradigms Workshop (NSPW), Annual Computer Security Applications Conference (ACSAC)

**2020** Symposium on Usable Privacy and Security (SOUPS), IEEE European Symposium on Security and Privacy (EuroS&P), IEEE Workshop on the Internet of Safe Things (SafeThings)

**2019** Usable Security Workshop (USEC), Symposium on Usable Privacy and Security (SOUPS), European Workshop on Usable Security (EuroUSEC), International Workshop on Socio-Technical Aspects in Security and Trust (STAST)

**2018** IEEE European Symposium on Security and Privacy (EuroS&P), Online Privacy and Data Security (OPDS), International Workshop on Socio-Technical Aspects in Security and Trust (STAST)

**2017** Symposium on Usable Privacy and Security (SOUPS), New Security Paradigms Workshop (NSPW), European Workshop on Usable Security (EuroUSEC), Cryptology and Network Security (CANS), International Workshop on Socio-Technical Aspects in Security and Trust (STAST)

**2016** Usable Security Workshop (USEC), New Security Paradigms Workshop (NSPW), European Workshop on Usable Security (EuroUSEC), International Conference on Passwords, International Workshop on Socio-Technical Aspects in Security and Trust (STAST)

**2015** New Security Paradigms Workshop (NSPW)

**Journal Reviewer:**

ACM Transactions on Privacy and Security
ACM Transactions on Multimedia Computing, Communications and Applications
ACM Transactions on Computer-Human Interaction
Communications of the ACM
Behaviour & Information Technology (Taylor & Francis)
Computers & Security (Elsevier)
IEEE Internet Computing
IEEE Security & Privacy
IEEE Transactions on Dependable and Secure Computing
IEEE Transactions on Information Forensics & Security
Interacting with Computers (Oxford University Press)

**Grant Reviewer:**

**2023** MITACS Accelerate Reviewer

**2020** Expert evaluator for "Bridge" R&D Funding Programme (Austrian Research Promotion Agency)

**2019** Expert evaluator for "Bridge Young Scientists" R&D Funding Programme (Austrian Research Promotion Agency)

**2017** Juror for "ICT of the Future" R&D Funding Programme (Austrian Research Promotion Agency)
Evaluated grant applications in the area of "Internet of Things - Safe, Secure, and Usable"

**Steering Committees:**

**2022–2025** Symposium on Usable Privacy and Security

**2020–Present** New Security Paradigms Workshop

**Leadership:**

**2014, 2016 – 2021** Who are you?! Adventures in Authentication: WAY Workshop Co-chair and organizer

**2017, 2019, 2021, 2022** John Karat Usable Privacy and Security Student Research Award Selection Committee Member

**2019–2020** NSPW Program Co-chair

**2018** CCS Posters Co-Chair

**2015 – 2017** SOUPS Lightning Talks and Demos Chair

**2015** NSPW Publicity Chair

**2013** ISSNet Summer Week Co-chair

**Thesis Committee Member:**

| | |
|---|---|
| **2022** | Veronica Chiarelli (M.Cog Sci), Sarah Moore (M.HCI), Khadija Baig (M.CS) |
| **2020** | Sandra Gabriele (M.HCI), Joshua Carr (M.HCI) |
| **2019** | Rebecca Jeong (M.HCI), Michael Lutaaya (M.CS), Alexandra Mesley (M.HCI), Jessica Rocheleau (M.HCI), and Daniela Ghanbari Vahid (M.HCI) |

**Defence Chair:**

| | |
|---|---|
| **2022** | Xuejun Han (PhD CS Proposal) |
| **2021** | Mohammad Zaeem (M.CS) |
| **2020** | Fiona Westin (M.HCI) |

**University Service:**

| | |
|---|---|
| **2022–2023** | Co-director, HCI Masters program<br>Carleton University Research Ethics Board B Committee Member |
| **2020–2021** | SCS Co-op Report Marker |
| **2019–2020** | SCS Hiring Committee (Tenure-Track Assistant Professor in AI/ML)<br>Institute of Cognitive Science Hiring Committee (1-yr Term Instructor)<br>SCS Co-op Report Marker |

---

## Presentations

| | |
|---|---|
| **2023** | **Making Security Memorable**<br>Invited presentation at Carleton Data Day 2023. Ottawa, Canada. |
| **2022** | **Remembering Your Passwords, One Picture at a Time**<br>Invited presentation in the Curiosity on Stage presenter series hosted by the Ingenium Foundation. Ottawa, Canada. |
| **2021** | **Password Sharing in Bangladesh**<br>Invited presentation in the iLab seminar series at University of Calgary. Calgary, Canada. Host: Dr. Helen Ai He |
| **2020** | **The Password Life Cycle**<br>Invited presentation in the CLUE seminar series at Carleton University. Ottawa, Canada. |
| **2018** | **Cybersecurity in Health Care**<br>Invited presentation at Emergency Preparedness in Healthcare Conference. Montreal, Canada. |
| | **Exploring the Usability of Two-factor Authentication**<br>Invited talk at Carleton University. Ottawa, Canada. Host: Dr. Paul van Oorschot. |
| | **The Password Life Cycle**<br>Invited talk at Polytechnique Montreal. Montreal, Canada. Host: Dr. Pierre Langlois. |
| **2017** | **Cognition-Informed Security**<br>Invited talk at McMaster University. Hamilton, Canada. Host: Dr. Ridha Khedri. |
| | **Cognition-Informed Security**<br>Invited presentation at Ruhr-Universität Bochum, Germany. Host: Dr. Thorsten Holz. |

**Coping with Passwords: Experts vs. Ordinary Users**
Invited conference presentation at Security and Human Behaviour Workshop. Cambridge, UK.

**Exploring the Usability of Two-factor Authentication**
Invited talk at Carnegie Mellon University. Pittsburgh, USA. Host: Dr. Lujo Bauer.

**Password-Based Protection of Privacy and Personal Data: friend or foe?**
Invited panelist at Computers, Privacy & Data Protection Conference (CPDP). Brussels, Belgium.

**2016** **Usable Security: From weakest link to powerful ally**
Invited speaker in the UBS Security Champions Training Series. Zürich, Switzerland.

**Exploring Website Location as a Security Indicator**
Invited talk at Technical University of Berlin, Germany. Host: Lydia Kraus

**What do users want from mobile authentication?** E. Stobert & R. Biddle.
Conference presentation at *Privacy Berlin 2016*. Berlin, Germany.

**The Psychology of Passwords**
Invited talk at University of Innsbruck, Austria. Host: Dr. Rainer Böhme

**2015** **The Password Life Cycle: How users and experts cope with passwords**
Invited talk at Ruhr-Universität Bochum, Germany. Host: Dr. Markus Duermuth

**Coping Strategies for Password Management**
Invited talk at University of Zürich, Switzerland. Host: Helen Ai He

**2014** **The Password Life Cycle**
Invited talk at ETH Zürich, Switzerland. Host: Dr. Srdjan Čapkun

**2013** **Memory Retrieval and Graphical Passwords**
Invited talk at University of New Brunswick, Canada. Host: Dr. Natalia Stakhanova

**A Password Manager that Doesn't Remember Passwords**
Conference presentation at *GRAND 2013*. Toronto, Canada.

**GREPSEC Workshop**
Participant in the GREPSEC Workshop for Women and Underrepresented Minorities working in Computer Security.

**2012** **Visual End-User Security**
Graduate Consortium, IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC). Innsbruck, Austria.

**User-Choice Patterns in PassTiles Graphical Passwords.**
Conference presentation at *GRAND 2012*. Montreal, Canada.

**2010** **Helping Users Build Mental Models of Computer Security**
Doctoral consortium, International Conference on Persuasive Technology. Copenhagen, Denmark.

**Usability and Strength in Click-based Graphical Passwords**
Invited talk at ACM SIGCHI Ottawa Chapter (CapCHI). Host: Dr. Andrew Patrick.

## Publications

**Refereed Journal Papers:**

**2021** **The EDIT Survey: Identifying Emergency Department Information Technology Knowledge and Training Gaps.** D. Kollek, D. Barrera, E. Stobert, & V. Homier.
*Disaster Medicine and Public Health Preparedness.* March 2021. doi: `https://doi.org/10.1017/dmp.2020.474`.

**2018** **Teaching Authentication as a Life Skill** E. Stobert, E. Cavar, L. Malisa, & D. Sommer.
*IEEE Security & Privacy Magazine.* September-October 2018. (5 pages)

**The Password Life Cycle.** E. Stobert & R. Biddle.
*ACM Transactions on Privacy and Security (TOPS).* April 2018. (30 pages)

**OmniShare: Encrypted Cloud Storage for the Multi-Device Era.** A. Paverd, S. Tamrakar, H.L. Nguyen, P.K. Pendyala, T.D. Nguyen, E. Stobert, T. Gröndahl, N. Asokan, & A-R. Sadeghi.
*IEEE Internet Computing.* April 2018. (7 pages)

**2012** **Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism.** S. Chiasson, E. Stobert, A. Forget, R. Biddle, & P.C. van Oorschot.
*IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2012. (15 pages)

**Refereed Conference Papers:**

**2023** **Security is a "Soft" Subject: Comparing Teacher and Creator Perspectives on the Design of Cybersecurity and Privacy Educational Resources** J. McLeod, L. Zhang-Kennedy, & E. Stobert. In submission to the *Symposium on Usable Privacy and Security (SOUPS 2023).*

**"This is different from the Western world": Understanding Password Sharing Among Young Bangladeshis** A. Alam, E. Stobert, & R. Biddle. *2023 Workshop on Usable Security and Privacy (USEC 2023). (February 2023)*

**2022** **"I look at them and it's like second nature. I don't really give them piece of mind": User Perceptions of Social Engineering Attacks** L. Kyi & E. Stobert. *2022 Symposium on Electronic Crime Research (eCrime 2022). (December 2022)*

**2021** **Authentication Management of Home IoT Devices.** A. Alam, H. Molyneaux & E. Stobert.
*Proceedings of the International Conference on Human-Computer Interaction (HCII 2021).* Springer LNCS. *(July 2021)*

**Emics and Etics of Usable Security.** A. Alam, R. Biddle & E. Stobert.
*Proceedings of the International Conference on Human-Computer Interaction (HCII 2021).* Springer LNCS. *(July 2021)*

**How Do Users Chain Email Accounts Together?** L. Kraus, M. Svidronova, & E. Stobert.
*Proceedings of the 36th International Conference on Information Security and Privacy Protection.* Springer LNCS. *(June 2021)*

**2020** **ByPass: Reconsidering the Usability of Password Managers** E. Stobert, T. Safaie, H. Molyneaux, A. Youssef & M. Mannan.
*Proceedings of the International Conference on Security and Privacy in Communication Networks (SecureComm 2020).* Springer LNCS. October 2020.

**Security Matters ... Until Something Else Matters More: Cybersecurity Awareness of Users on Device Form Factors.** H. Molyneaux, E. Stobert, I. Kondratova, & M. Gaudet. *Proceedings of the International Conference on Human-Computer Interaction (HCII 2020).* Springer LNCS. August 2020

**[Short Paper] How Individual Differences Impact Perceived Password Management.** L. Kyi, S. Chiasson, & E. Stobert.
*Proceedings of Who Are You?!: Adventures in Authentication Workshop (WAY 2020).* Virtual Conference. August 2020.

**Understanding Cybersecurity Practices in Emergency Departments** E. Stobert, D. Barrera, V. Homier, & D Kollek.
*Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI 2020).* ACM. April 2020.

**2019** **Work in Progress: A Comparative Long-Term Study of Fallback Authentication** P. Markert, M. Golla, E. Stobert & M. Duermuth.
*Proceedings of the NDSS Workshop on Usable Security 2019 (USEC).* Internet Society. February 2019.

**Understanding Perceptions: User Responses to Browser Warning Messages** H. Molyneaux, I. Kondratova, & E. Stobert.
*Proceedings of the International Conference on Human-Computer Interaction (HCII 2019).* Springer LNCS. August 2019.

**2018** **Exploring Website Location as a Security Indicator.** D.Y. Yu, E. Stobert, D. Basin, & S. Capkun.
*Proceedings of the NDSS Workshop on Usable Security 2018 (USEC).* San Diego, USA. Internet Society. February 2018. (34% acceptance rate)

**2017** **Teaching Authentication in High Schools: Challenges and Lessons Learned.** E. Stobert, E. Cavar, L. Malisa & D. Sommer.
*Proceedings of the 2017 USENIX Workshop on Advances in Security Education*, Vancouver, Canada. USENIX. August 2017.

**2016** **Mobile Device Security: Hopes and Fears.** E. Stobert, I. Reyes, C. Gates, & R. Biddle.
*Proceedings of the 10th International Conference on Passwords*, Bochum, Germany. LNCS. December 2016.

**[Short Paper] Picking a (Smart)Lock: Locking Relationships on Mobile Devices.** E. Stobert & D. Barrera.
*Proceedings of Who Are You?!: Adventures in Authentication Workshop (WAY)*, Denver, USA. June 2016.

**2015** **Expert Password Management.** E. Stobert & R. Biddle.
*Proceedings of the 9th International Conference on Passwords*, Cambridge, UK. LNCS. December 2015. (33% acceptance rate, winner of the best paper award)

**A First Look at the Usability of Bitcoin Key Management.** S. Eskandari, D. Barrera, E. Stobert & J. Clark.
*Proceedings of the NDSS Workshop on Usable Security 2015 (USEC)*, San Diego, USA. Internet Society. February 2015. (38% acceptance rate)

**2014** **A Password Manager that Doesn't Remember Passwords.** E. Stobert & R. Biddle.
*Proceedings of the New Security Paradigms Workshop (NSPW)*, Victoria, Canada. ACM. September 2014. (30% acceptance rate)

**The Password Life Cycle: User Behaviour in Managing Passwords.** E. Stobert & R. Biddle.
*Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, Menlo Park, USA. USENIX. July 2014. (27% acceptance rate)

**2013** **Memory Retrieval and Graphical Passwords.** E. Stobert & R. Biddle.
*Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, UK. ACM. July 2013. (29% acceptance rate)

**[Short Paper] Authentication in the Home.** E. Stobert & R. Biddle.
*Proceedings of the Workshop on Home Usable Privacy and Security (HUPS)*, Newcastle, UK. July 2013.

**2012** **[Short Paper] The MVP Web-based Authentication Framework.** S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan, R. Biddle.
*Proceedings of Financial Cryptography (FC)*, Bonaire. LNCS. February 2012. (33% acceptance rate)

**2010** **Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords.** E. Stobert, A. Forget, S. Chiasson, P.C. van Oorschot & R. Biddle.
*Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, Austin, USA. ACM. December 2010. (16% acceptance rate)

**2009** **Multiple Password Interference in Text and Click-based Graphical Passwords.** S. Chiasson, A. Forget, E. Stobert, P.C. van Oorschot & R. Biddle.
*Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Chicago, USA. ACM. November 2009. (18% acceptance rate)

**Refereed Posters:**

**2020** **Etics and Emics of Usable Security: Culturally Universal or Culturally Specific?** A. Alam, R. Biddle & E. Stobert.
*2020 SERENE-RISC Workshop*, Virtual Conference. October 2020.

- Best poster winner.

**Something Doesn't Feel Right: Using Thermal Warnings to Improve User Security Awareness.** D. Napoli, S. Navas Chaparro, S. Chiasson, & E. Stobert.
*Symposium on Usable Privacy and Security (SOUPS)*, Virtual Conference. USENIX Association. August 2020.

**2015** **How Do Experts Manage their Passwords?** E. Stobert & R. Biddle.
*Symposium on Usable Privacy and Security (SOUPS)*, Ottawa, Canada. USENIX Association. July 2015.

**2014** **The Agony of Passwords: Can we learn from user coping strategies?** E. Stobert.
*ACM Conference on Human Factors in Computing Systems (CHI)*, Toronto, Canada. ACM. April 2014.

- Semi-finalist in the international student research competition.

**2010** **Persuasion, Social Graces, and Computer Security.** E. Stobert, S. Chiasson & R. Biddle.
*5th International Conference on Persuasive Technology*, Copenhagen, Denmark. LNCS. June 2010.

**Usability and Strength in Click-based Graphical Passwords.** E. Stobert.
*ACM Conference on Human Factors in Computing Systems (CHI)*, Atlanta, USA. ACM. April 2010.

- $3^{rd}$ place finalist in the international student research competition

**Theses:**

**2015** **Graphical Passwords and Practical Password Management**
**E. Stobert**.
School of Computer Science, Carleton University, Ottawa, Canada. May 2015.

**2011** **Memorability of Assigned Random Graphical Passwords**
**E. Stobert**.
Department of Psychology, Carleton University, Ottawa, Canada. August 2011.

---

## References

References available upon request

16 May 2023

**Paul C. Van Oorschot, FRSC**
http://www.scs.carleton.ca/~paulv/

**I.** **Paul Van Oorschot**. Professor (tenured), School of Computer Science
Carleton University, 1125 Colonel By Drive, Ottawa, Canada K1S 5B6
Canada Research Chair (Tier I) in Authentication and Computer Security
Member of Graduate Faculty, Ottawa-Carleton Institute for Computer Science (OCICS)

## II. EARNED DEGREES:

Ph.D. (1988, Computer Science), University of Waterloo, Canada.
Thesis: *Combinatorial and Computational Issues Related to Finding Roots of Polynomials Over Finite Fields*

M.Math. (1986, Computer Science), University of Waterloo, Canada.
Thesis: *Algorithms for Cryptosystems Using Modular Exponentiation*

B.Math. (1984, Honours, Computer Science), University of Waterloo, Canada.

## III. APPOINTMENTS / EMPLOYMENT HISTORY:

2002- Professor, School of Computer Science, Carleton University, Ottawa
2002-2002 Chief Scientist & Principal Research Associate (2002-03), Cloakware Corp, Ottawa
1997-2001 VP / Chief Scientist / Chief Security Architect, Entrust Technologies, Ottawa
1994-1996 Senior Scientific Advisor (Entrust Group), Bell-Northern Research, Ottawa
1993-1994 University Visitor, School of Computer Science, Carleton University
1992-1994 Cryptographic Consultant (Secure Networks), Bell-Northern Research, Ottawa
1991-2002 Adjunct Research Professor, School of Computer Science, Carleton University
1988-1992 Scientific Staff (Division 7/Central Switching), Bell-Northern Research, Ottawa
1987-1987 (Jan.-Apr.) Instructor, Faculty of Mathematics, University of Waterloo, Canada
1981-1984 (summers) Compiler Writer/Systems Programmer, WATCOM, Waterloo, Canada

## IV. ACADEMIC HONOURS, AWARDS, DISTINCTIONS (including non-academic):

2019 IEEE Fellow, "for contributions to applied cryptography and authentication"
2019 Co-author, Best Paper, PST 2019, Fredricton, NB.
2018 Co-author, Best Paper, IEEE SecDev 2018, Cambridge, MA.
2017-2022 Professorial Fellow (Hon. Prof.), Univ. Melbourne, School of Computing & Info Systems
2017 Co-author, Distinguished Paper, AsiaCCS (Comp. & Comm. Security), Abu Dhabi
2016 ACM Fellow, "for contributions to applied cryptography, authentication, computer security"
2016-2023 Canada Research Chair in Authentication and Computer Security
2013 Faculty Graduate Mentoring Award, Carleton University
2012 Co-author, Best Student Paper, ISC (Information Security Conference), Germany
2011 Fellow of Royal Society of Canada (FRSC),
Academy III/Science (Mathematics and Physical Sciences)

2009-2016 Canada Research Chair in Internet Authentication and Computer Security
2002-2009 Canada Research Chair in Network and Software Security
2007 Co-author, Best Paper, SOUPS (Symposium on Usable Privacy and Security)
2007 Co-author, Outstanding Paper, ACSAC (Annual Computer Security Applic. Conf.)
2001 J.W. Graham Medal in Computing & Innovation (Univ. of Waterloo). *Awarded annually to an alumnus who exemplifies the qualities shown by Wes Graham during his career.*
1986-1988 Member of Board of Governors, University of Waterloo
1986-1988 Member of University Senate, University of Waterloo
1986-1988 Petro-Canada Inc. Graduate Research Award
1984-1988 NSERC Postgraduate Scholarship
1984-1988 NSERC "1967" Science & Engineering Scholarship (declined)
1984 Ontario Graduate Scholarship (declined)
1984 K.D. Fryer Gold Medal. First recipient. *Presented annually to a graduating University of Waterloo Math student who best exemplifies academic excellence and good student citizenship.*
1984 Graduated on Dean's Honors list, 93.9% undergraduate average.
Class rank 1980-81: 1/254, 1981-82: 1/215, 1982-83: 1/256.
1980-1984 Ford Motor Company of Canada Scholarship
1980-1984 Univ. Waterloo Athlete of Year (1982-83), Most Valuable Player (basketball 1982-83), varsity captain 1982-84, national finalists 1982-83, semi-finalists 1983-84.
1980 Univ. Waterloo Descartes Fellowship. Rhodes Scholarship Candidate (1983).
1980 Ontario Scholar, Valedictorian (Milton District HS). Final year grade average 99.6%.

## V. INDUSTRIAL POSITIONS (DETAILS):

**Cloakware Corporation (now Irdeto Canada)** (Mar.2002-Aug.2002: Chief Scientist)
Private software security firm providing software obfuscation technology and services, to counter software tampering and reverse engineering of proprietary software. Scientific lead on research in software tamper-resistance and automated code transformation tools. Participation in corporate financing activities, strategic planning, internal consulting. Principal Research Associate (2002–2003); Board of Advisors (2001-2002).

**Entrust Technologies, Ottawa** (Jan.1997-Nov.2001; on leave Dec.2001-Feb.2002)
Chief Scientist / Chief Security Architect / Vice-President. Internet security software firm, 800 employees (Jun.2002). Annual revenue US$118 million (2001). Participated in August 1998 IPO (Nasdaq:ENTU), following January 1997 spin-out from Northern Telecom. One of six founding employees (1993). Experienced growth to 1200 employees (1Q2001). Pioneered "Public Key Infrastructure (PKI)", a US$500 million market category in 2002. Initiated and grew intellectual property program, yielding over 90 U.S. patents/patents pending. Designed advanced security architectures, cryptographic protocols. Initiated security assurance program. Led international security standards initiatives (encryption, authentication, digital signatures). Advised on national and international cryptographic policy and cryptographic export controls.

**Bell-Northern Research (BNR) and Northern Telecom, Ottawa** (Sept.1988-Dec.1996)
Sr Scientific Advisor/Cryptographic Consultant/Scientific Staff, Secure Networks Group. Lead architect, Entrust PKI product for cross-platform privacy & authentication (1993-96). Design of Canadian government-wide electronic key management system (1993-1995).

Design and development, X.25 packet data network security crypto module (1989-92).
Establishment of cryptographic center of expertise for Northern Telecom and subsidiaries.
Security planning for European GSM digital cellular network (1992-1993).
Participation in U.S. National Security Agency classified ISDN Security Program (1992).
Security consulting in wireless communications, international standards forums.

## VI. SCHOLARLY AND PROFESSIONAL ACADEMIC ACTIVITIES:

**SCS Service:**

2022-2023: Developed new undergrad course COMP2109 (Introduction to Security and Privacy)
2021-2023: Progressing proposed (new) Bach. Computer and Internet Security (BCIS) program (activity led by Doug Howe, also with Michel Barbeau)

**Fifteen Contributions Exemplifying Significance and Impact** (full publications: see further below)
[n] indicates item in full list below. GS = number of Google Scholar citations per 16 May 2023.

i) *Handbook of Applied Cryptography* ([1] CRC 1996; GS =23,480) Encyclopedic treatment of applied cryptography. Turing Award winner Rivest's foreword calls it "a landmark in the development of the field".

ii) "Parallel collision search with cryptanalytic applications" ([48] J.Crypt 1999; GS=840) Introduced a fully parallelizable generic search algorithm directly affecting security of digital signature, cryptographic hash function, and discrete logarithm-based cryptosystems; impacted design of numerous subsequent algorithms.

iii) "On the security of iterated message authentication codes" ([49]; IEEE-IT 1999; GS=122) Novel cryptanalysis showed generic weaknesses in using iterated hash functions for MACs (Message Authentication Codes); resulted in retraction of international banking authentication standards, and influenced later MAC designs.

iv) "Authentication and authenticated key exchanges" ([53] DCC 1992; GS=1,675) Explication of the STS key establishment protocol; influenced both theory and practice; variations later adopted in IETF, ISO standards.

v) "On Diffie-Hellman key agreement with short exponents" ([143] Eurocrypt'96; GS=224) Cryptanalysis showing security weaknesses resulting from attempts to speed-up algorithms by using too-short keys; provided algorithmic justification for the now-standard practice of using large prime-order subgroups in key exchange.

vi) "On unifying some cryptographic protocol logics" ([147] Oakland 1994; GS=510) Introduced the SVO logic, unifying three BAN-family authentication logics with another (from [146]) that was the first logic capable of formal reasoning about key agreement algorithms such as Diffie-Hellman.

vii) "On predictive models and user-drawn graphical passwords" ([42] TISSEC 2008; GS=179) First generic approach for cryptanalysis of graphical password schemes, debunking belief that they offered greater security than text passwords.

viii) "Graphical passwords: Learning from the first twelve years" ([26] CSur 2012; GS=923) Systematization giving scientific footing to graphical password research; through combined user studies and novel cryptanalysis, showed graphical schemes have largely similar characteristics and drawbacks as traditional password schemes.

ix) "SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements" ([75] Oakland 2013; GS=318) Systematized research on public-key infrastructures/PKI supporting the TLS security mechanism in browser-server HTTPS; contributed to resurgence in PKI proposals

aiming to replace current Internet infrastructure whereby all users rely on certificates issued by commercial Certification Authorities.

x) "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes" ([80] Oakland 2012; GS=1,275) Introduced a now-benchmark framework and process for evaluating user authentication proposals; recognized deployability as a major dimension, and criteria to measure it.

xi) "An administrator's guide to Internet password research" ([69] LISA 2014; GS=217) Systematic re-examination of password best practices; uncovered misconceptions, introduced "online-offline gap"; together with related contributions [20,71,18,19,28], resulted in major changes in revised US, UK government password guidelines.

xii) "White-box cryptography and an AES implementation" ([138] SAC 2002; GS=605) Along with [139], the first two papers introducing and illustrating white-box cryptography, a generic method of software obfuscation for cryptographic keys, now in wide commercial use and spawning an ongoing active research area.

xiii) "A generic attack on checksumming-based software tamper resistance" ([128] Oakland 2005; GS=158) Novel cryptanalytic method defeating all methods in a then-commonly used software tamper resistance approach.

xiv) "Internet geolocation: Evasion and counter-evasion" ([40] CSur 2009; GS=199) Initiated the research field exploring methods for determining the geographic location corresponding to an Internet presence, in the case where there is direct intent to evade being accurately located; now a mainstream research area [17,14,16,63].

xv) "Science, security, and the elusive goal of security as a scientific pursuit" ([62] Oakland 2017; GS=113) Critical analysis of U.S. government "Science of Security" agenda, and relationship between crypto-security research and science as practiced over the past few centuries.

**Leadership in Canadian Academia and Canadian Security Research Networks:**

2017-2018 Advisory Board member, Canadian Institute for Cybersecurity (UNB, Fredericton)
2013-2017 New Fellows Selection Committee, RSC Academy III (Math & Physical Sciences)
2008-2014 Scientific Director/Principal Investigator, NSERC Internetworked Systems Security Network (ISSNet), $5m Strategic Network Grant, 15 professors across 8 universities
2005-2009 MITACS Project Leader (Mitigating Malicious Computer Network Activity)
2002- Founder and Director, Carleton Computer Security Laboratory, Carleton University

**Program Committee Member, Major International Conferences and Workshops:**

2016: Passwords 2016, Ruhr-University Bochum, Germany
2016: New Security Paradigms Workshop (NSPW), Colorado, USA
2015: Passwords 2015, Cambridge, UK
2015: New Security Paradigms Workshop (NSPW), Twente, Netherlands
2014: New Security Paradigms Workshop (NSPW), Victoria, BC, Canada
2013: 9th Symposium on Usable Privacy and Security (SOUPS), Newcastle, UK
2013: New Security Paradigms Workshop (NSPW), Banff, Canada
2012: New Security Paradigms Workshop (NSPW), Bertinoro, Italy
2011: 18th ACM Conference on Computer & Communications Security (CCS), Chicago, Illinois
2011: ACM CCS Workshop on Security & Privacy in Smartphones and Mobile Devices, Chicago
2010: 6th Symposium on Usable Privacy and Security (SOUPS), Redmond, Washington

2010: 5th USENIX Hot Topics in Security (HotSec), Washington D.C.
2009: 16th ACM Conference on Computer and Communications Security (CCS), Chicago
2009: 5th Symposium on Usable Privacy and Security (SOUPS), Mountain View, California
2008: 17th USENIX Security Symposium, San Jose, California
2008: 15th ACM Conference on Computer and Communications Security, Alexandria, Virginia
2008: New Security Paradigms Workshop, Lake Tahoe, California
2008: Usability, Psychology and Security (UPSEC'08), San Francisco, California
2007: 28th IEEE Symposium on Security and Privacy, Berkeley/Oakland, California
2007: Usable Security (USEC'07), Scarborough, Trinidad & Tobago
2007: New Security Paradigms Workshop, North Conway, New Hampshire
2007: 3rd Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, Pennsylvania
2007: 16th USENIX Security Symposium, Boston, Massachusetts
2007: 23rd ACSA Annual Computer Security Applications Conference, Miami Beach, Florida
2007: 3rd USENIX Steps to Reducing Unwanted Traffic on the Internet (SRUTI'07), Santa Clara
2006: 27th IEEE Symposium on Security and Privacy, Berkeley/Oakland, California
2006: 26th IEEE Int'l Conf. on Distributed Computing Systems (ICDCS), Lisboa, Portugal
2006: 1st USENIX Hot Topics in Security, Vancouver, Canada
2006: New Security Paradigms Workshop, Dagstuhl, Germany
2005: 14th USENIX Security Symposium, Baltimore, Maryland
2005: 21st ACSA Annual Computer Security Applications Conference, Tucson, Arizona
2005: 3rd ACM Workshop on Rapid Malcode (WORM'05), Fairfax, Virginia
2004: 13th USENIX Security Symposium, San Diego, California
2004: 11th Annual Network and Distributed System Security Symposium (NDSS), San Diego
2003: Eurocrypt 2003, Warsaw, Poland
2003: 6th International Information Security Conference (ISC-6), Bristol, U.K.
2003: 3rd Annual ACM Workshop on Digital Rights Management, Washington, D.C.
2003: 10th Annual International Workshop on Selected Areas in Cryptography, Ottawa, Canada
2002: 9th Annual Network and Distributed System Security Symposium (NDSS), San Diego
2002: Eurocrypt 2002, Amsterdam, Netherlands
2001: 8th Annual Network and Distributed System Security Symposium (NDSS), San Diego
2000: 7th Annual Network and Distributed System Security Symposium (NDSS), San Diego
2000: Eurocrypt 2000, Bruges, Belgium
2000: 20th Annual International Cryptology Conference (Crypto 2000), Santa Barbara, California
1999: Eurocrypt'99, Prague, Czech Republic
1999: Communications and Multimedia Security (CMS'99)
1998: 5th ACM Conference on Computer and Communications Security, San Francisco
1997: Eurocrypt'97, Konstanz, Germany
1996: 3rd ACM Conference on Computer and Communications Security, New Delhi, India
1996: 16th Annual International Cryptology Conference (Crypto'96), Santa Barbara, California
1996: AsiaCrypt, Kyongju, Korea
1995: 2nd International Workshop on Selected Areas in Cryptography, Ottawa, Canada
1994: 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia
1993: 1st International Workshop on Selected Areas in Cryptography, Kingston, Ontario

**Leadership in International Security and Cryptography Community:**

2022 May External examiner, PhD candidate Martin Ukrop (advisor: V. Matyas), Masaryk U
2021- Dept. Editor (Security Knowledge), *IEEE Security and Privacy*

| | |
|---|---|
| 2019 Sept | Guest co-editor, Special Issue (IoT Security), *IEEE Security & Privacy* 17(5). |
| 2019 Jan. | External examiner, PhD candidate Udyani Herath (advisor: D. Stebila), QUT Australia |
| 2018-2021 | Associate Editor-in-Chief, *IEEE Security and Privacy* |
| 2018 Jan. | External examiner, PhD candidate Ildar Muslukhov (advisor: Kosta Beznosov), UBC |
| 2017 | Editor-in-Chief Search Committee*, IEEE Security & Privacy* |
| 2017 | Distinguished Expert Review Team, NSA Best Scientific Cybersecurity Paper |
| 2017-2017 | Associate Editor, *IEEE Security and Privacy* |
| 2016 July | External examiner, PhD candidate Hassan Khan (advisor: U. Hengartner), Waterloo |
| 2015 Nov. | Member of international team of 12 charged to review the Dept of Computer Science of the Swiss Federal Institute of Technology, Zurich (ETH-Zurich) |
| 2015 May | External examiner, PhD candidate Saranga Komanduri (advisor: L. Cranor), CMU |
| 2014 Dec. | External examiner, PhD candidate Joel Reardon (advisor: David Basin), ETH-Zurich |
| 2014-2015 | Program Chair, New Security Paradigms Workshop (2014 Jr chair, 2015 Sr chair) |
| 2013 Nov. | External examiner, PhD candidate San-Tsai Sun (advisor: Kosta Beznosov), UBC |
| 2011-2014 | Associate Editor, *IEEE Trans. on Dependable and Secure Computing* (IEEE TDSC) |
| 2011-2014 | Associate Editor, *IEEE Trans. on Information Forensics & Security* (IEEE TIFS) |
| 2011 | Co-chair, FC 2011 workshop on the Future of User Authentication on the Web |
| 2010 | General Co-chair, IEEE Workshop on Information Forensics & Security, Seattle |
| 2008 | Program Chair, USENIX Security, San Jose, California |
| 2007 | External examiner, PhD candidate Ronald W. Smith (advisor: S. Knight), Queen's U. |
| 2007 | External examiner, PhD Jasvir Nagra (advisor: C. Thomborson), U. Auckland, NZ |
| 2005-2011 | Associate Editor, *ACM Trans on Information and System Security* (ACM TISSEC) |
| 2005-2006 | Board of Directors, Forum for Information Security Innovation in Canada (FISIC) |
| 2002-2006 | Steering Group, Internet Society NDSS Symposium (San Diego) |
| 2002 | Program Chair (senior), Internet Society NDSS Symposium, San Diego, California |
| 2001 | Program Chair (junior), Internet Society NDSS Symposium, San Diego, California |
| 1996-2010 | Associate Editor, *Designs, Codes and Cryptography* (DCC), Kluwer Academic |
| 1993-2001 | Board of Directors, International Association for Cryptologic Research (IACR) |
| 1999-2001 | Board of Directors, Security Research Alliance (representing Entrust Technologies) |
| 1998 | Board of Directors, Key Recovery Alliance (lead by IBM Corporation) |
| 1995 | Program co-Chair, 2nd International Workshop on Selected Areas in Cryptography |
| 1990-1998 | Canadian and/or Bell-North Research representative to standardization bodies:<br>ISO/SC27 Standards (Information Technology–Security Techniques),<br>ANSI X9F (Financial Services–Data and Information Security),<br>TIA TR45.3: North American Digital Cellular–Authentication and Privacy |
| 1993 | General Chair, Crypto'93, Santa Barbara, California |
| 1992 | External examiner, PhD candidate Glenn A. Orton (advisor: S. Tavares), Queen's U. |

## VII. GRADUATE THESES SUPERVISED AND POSTDOCS HOSTED

Completed (summary statistics): 11 Masters, 13 PhD, 10 Postdoctoral
In progress (summary statistics): 2 PhD

**In-progress theses (grad student supervisions)** (‡denotes as secondary advisor)

| | | | |
|---|---|---|---|
| PhD | Vathsan Morkonda‡ | Jan 2021 - | authentication (main advisor: S. Chiasson) |
| PhD | Ali Jahromi‡ | Jan 2022 - | network security (main advisor: A. Abdou) |

**Masters theses supervised (as primary research supervisor)** (‡denotes as secondary advisor)

Christopher Bennett (Jan.2019-Jan.2021)
- *Search Engines that Scan for Internet-Connected Services: Classification and Empirical Study*

Reza Semanfar (Sept.2017-Jun.2020)
- *Binding Social Identity with Email Address and Automating Email Certificate Issuance*

Hemant Gupta (Sept.2017-Aug.2019)
- *Onboarding and Software Update Architecture for IoT Devices*

Daniel McCarney (Sept.2011-Aug.2013)
- *Password Managers: Comparative Evaluation, Design, Implementation, Analysis*

Carson Brown‡ (Sept.2008-Dec.2010)
- *A Meta-Scheme for Authentication using Text Adventures*

David Barrera (Jan.2008-Aug.2009)
- *Towards Classifying and Selecting Appropriate Security Visualization Techniques*

Jennifer Sobey (Sept.2006-Aug.2008)
- *An Evaluation of New Browser Indicators for Extended Validation Certificates*

Tim Furlong (Sept.2005-Apr.2007)
- *Tools, Data, and Flow Attributes for Understanding Network Traffic without Payload*

James Kelly (Sept.2004-Aug.2006)
- *An Examination of Pattern Matching Algorithms for Intrusion Detection Systems*

Mohammad Mannan (Sept.2003-Aug.2005)
- *Secure Public Instant Messaging*

Glenn Wurster (Sept.2003-April 2005)
- *A Generic Attack on Hashing-based Software Tamper Resistance*

**PhD theses supervised (as primary research supervisor)** (‡equal co-supervision)

Chris Bellman (Sept 2017 - Aug 2022)
- *On Security Best Practices, Systematic Analysis of Security Advice, and Internet of Things Devices*

Furkan Alaca (Sept 2012 - May 2018)
- *Strengthening Password-Based Authentication Through Multiple Supplementary Mechanisms*

AbdelRahman M. Abdou‡ (Sept.2011-Aug.2015). Co-advisor: A. Matrawy (SCE, Carleton)
- *Internet Location Verification: Challenges and Solutions*

Gerado Reynaga (secondary advisor, Sept.2009-Aug.2015). Co-advisor: S. Chiasson
- *The Usability of Captchas on Mobile Devices*

David Barrera (Sept.2009-July 2014)
- *Securing Decentralized Software Installation and Updates*

Mansour Alsaleh (Sept.2006-Dec.2011)
- *Defenses Against Network Scanning and Other Malicious Remote Host Activity*

Glenn Wurster (May 2005-Apr.2010)
- *Security Mechanisms and Policy for Mandatory Access Control in Computer Systems*

Mohammad Mannan (Sept.2005-Apr.2009)
- *Authentication and Securing Personal Information in an Untrusted Internet*

Sonia Chiasson‡ (Sept.2005-Dec.2008). **Senate Medal, Outstanding Academic Achievement**
- *Usable Authentication And Click-Based Graphical Passwords*

David Whyte (Sept.2002-Aug.2008)
- *Network Scanning Detection Strategies for Enterprise Networks*

Julie Thorpe (Jan.2003-Dec.2007). **Senate Medal, Outstanding Academic Achievement**

- *On the Predictability and Security of User Choice in Passwords*

Tao Wan (Sept. 2001-Dec.2005)

- *Securing Routing Protocols through Information Corroboration*

Mike Just (1995-1998)

- *On the Temporal Authentication of Digital Data*

**Post-Doctoral: PDF=Fellows (≥1 year), PDRA=Research Associates (>4 months) hosted**

Xavier de Carné de Carnavalet (2019-2020), PDF: network infrastructure security
A. Abdou (2015-2017), PDF: Internet authentication; network/system security
Jeremy Clark (2011-2013), PDF: authentication, usability and system security
Glenn Wurster (2010), PDRA: systems security
Sonia Chiasson (2009), PDF: graphical passwords and usable security
Tara Whalen (2009), PDRA: usability and security
Hajime Inoue (2005-2007), PDF: traffic classification (co-hosted)
James Muir (2005-2007), PDF: Internet geo-location, anonymity
Deholo Nali (2005-2007), PDF: authentication and privacy
Miguel Vargas Martin (Jan.2003-Jul.2004), PDF: worm detection in the Internet core

**Trainees who have secured university faculty positions**

| Trainee supervised | Period | Current University | Current Faculty Position |
|---|---|---|---|
| Mike Just | PhD | Heriot-Watt Univ. (UK) | Assoc. Prof./Deputy Head (Math/CS) |
| M. Vargas Martin | PDF | Univ. of Ontario (UOIT) | Professor |
| Julie Thorpe | PhD | Univ. of Ontario (UOIT) | Assoc. Professor |
| Sonia Chiasson | PhD/PDF | Carleton University | Professor |
| M. Mannan | PhD | Concordia U. (Montreal) | Assoc. Professor |
| Jeremy Clark | PDF | Concordia U. (Montreal) | Assoc. Professor, NSERC Res. Chair |
| Mansour Alsaleh | PhD | KACST (Saudi Arabia) | Asst. Professor |
| David Barrera | PhD | Carleton University | Asst. Professor |
| Furkan Alaca | PhD | Queen's University | Asst. Professor |
| A. Abdou | PhD/PDF | Carleton University | Asst. Professor |
| Xavier de Carnavalet | PDF | Hong Kong Polytechnic | Research Asst. Professor |

**Graduate Courses (last 8 years):**

2022 Jan-Apr COMP5407: Authentication and Software Security
2020 Sep-Dec COMP5900: Security and the Internet of Things
2019 Sep-Dec COMP5900: Security and the Internet of Things
2019 Jan-Apr COMP5407: Authentication and Software Security
2018 Jan-Apr COMP5407: Authentication and Software Security
2017 Jan-Apr COMP5407: Authentication and Software Security
2015 Jan-Apr COMP5407: Authentication and Software Security

**Undergraduate Courses (last 8 years):**

2023 Jan-Apr COMP2109: Introduction to Security and Privacy
2020 Sep-Dec COMP4108: Computer Systems Security
2019 Jan-Apr COMP4108: Computer Systems Security

2017 Jan-Apr COMP4108: Computer Systems Security

## VIII. EXTERNAL RESEARCH FUNDING (university career, 2002-2023):

*Type: C-Granting councils; G-Government; F-Foundations; O-Other

| | Year | Source | Type* | Amnt/yr | Purpose** |
|---|---|---|---|---|---|
| Current | | | | | |
| | 2018-2024 | NSERC (Discovery Grant) | C | $330,000 | operating grant, total over 6 years |
| | 2016-2023 | Canada Research Chair | G | $1,400,000 | support of research chair, over 7 years |
| Previous | | | | | |
| | 2019-2021 | DND/NSERC DG supplement | C | $120,000 | operating grant, total over 3 years |
| | 2009-2016 | Canada Research Chair | G | $1,400,000 | support of research chair |
| | 2002-2009 | Canada Research Chair | G | $1,400,000 | support of res. chair, NSERC CRC |
| | 2013 | NSERC ISSNet [Note 2] | G | $750,000 | research grant, extended to year 6 |
| | 2008-2013 | NSERC ISSNet [Note 2] | G | $5,000,000 | research grant, total over 5 years |
| | 2013-2018 | NSERC (Discovery Grant) | C | $220,000 | operating grant, total over 5 years |
| | 2008-2013 | NSERC (Discovery Grant) | C | $240,000 | operating grant, total over 5 years |
| | 2008-2011 | NSERC (Disc. Accelerator) | C | $120,000 | operating grant, total over 3 years |
| | 2003-2008 | NSERC (Discovery Grant) | C | $215,000 | operating grant, total over 5 years |
| | 2007-2009 | MITACS NCE [Note 1] | F | $100,000 | RA, student travel, total over 3 yrs |
| | 2007 | Communications Security Est. | G | $23,000 | research grant #4 |
| | 2007-2008 | Res. in Motion [Note 1] | O | $100,000 | research grant, total over 2 years |
| | 2006 | Commns Security Est. [Note 1] | G | $23,275 | research grant #3 |
| | 2006 | Commns Security Est. [Note 1] | G | $23,128 | research grant #2 |
| | 2006 | ORNEC/OCE ID Theft Project | G | $35,000 | research grant, total over 2 years |
| | 2005-2006 | MITACS NCE [Note 1] | F | $70,000 | RA, student travel, sem. series, 2 yrs |
| | 2005 | Bell University Labs | O | $15,000 | research grant |
| | 2005 | Commns Security Establishment | G | $23,500 | research grant #1 |
| | 2004 | MITACS NCE (seed) | F | $23,000 | RA, student travel |
| | 2003 | NCIT | F | $30,000 | RA |
| | 2003-2004 | Alcatel Canada | O | $95,000 | research grant, total over 2 years |
| | 2003-2004 | Cloakware Corp. | O | $30,000 | RA, general research, total 2 years |
| | 2003 | CFI (40%), OIT (40%) | F | $343,000 | infrastructure, CCSL |
| | | Bell, IBM, Cloakware (20%) | O | | (industry contribution to CFI total) |

**Note 1: Principal Investigator; along with co-Investigator at Carleton University

**Note 2: Principal Investigator & Sci. Director; shared with 14 supporting co-Investigators; 5+1 yr program, total funding $5 million (NSERC) + $750,000 partner funding

## IX. PUBLICATIONS (*Life-time summary).*

*Total citations 46,850; h-index 83* (16 May 2023) [http://scholar.google.ca/citations?user=CMRzTi8AAAAJ](http://scholar.google.ca/citations?user=CMRzTi8AAAAJ)

- Books authored…….3
- Books edited…….4
- Books chapters .....…….……..5
- Papers in refereed journals (under review)……....……52 (2)
- Papers in refereed conference proceedings …….…….. 100
- Other publications …….....…….....…….…….....28
- Technical reports and manuscripts, unpublished …….....7
- U.S. Patents + Canadian patents…...…….…….……18+2

*Details according to the above categories are given below. Convention used in ordering co-author names: for periodicals, authors listed alphabetically following customs in mathematical sciences; for conferences, students/trainees listed first followed by senior authors in alphabetical order, following customs in computer systems community. Inventor names on patents are listed principal inventor first, equal contributors alphabetically, in accordance with USPTO rules.*

**Books, authored:**

1. P.C. van Oorschot. *Computer Security and the Internet: Tools and Jewels*, Springer Nature (2020), 365 pages. Second Edition: *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*, Springer (2021), 446 pages.
2. A.J. Menezes, P.C. van Oorschot, S. Vanstone. *Handbook of Applied Cryptography*, CRC Press (1996), 780 pages.
3. S.A. Vanstone, P.C. van Oorschot. *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic Publishers (1989), 289 pages.

**Books or proceedings, edited:**

4. A. Somayaji, P.C. van Oorschot, M. Mannan, R. Böhme. Proc. 2015 New Security Paradigms Workshop (NSPW), Twente, The Netherlands, September 8-11, 2015. ACM 2015, ISBN 978-1-4503-3754-0.
5. K. Beznosov, A. Somayaji, T. Longstaff, P.C. van Oorschot. Proc. 2014 New Security Paradigms Workshop (NSPW), Victoria, BC, Canada, Sept 15-18, 2014. ACM 2014, ISBN 978-1-4503-3062-6.
6. P.C. van Oorschot (editor). Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA USENIX Association 2008.
7. E. Kranakis, P.C. van Oorschot (editors). *Selected Areas in Cryptography*, Kluwer Academic Publishers (1997), 108 pages, ISBN 0-7923-8023-1. Invited subset of papers from Selected Areas in Cryptography, 1995 (SAC'95).

**Books, chapters in:**

8. P.C. van Oorschot. Public Key Cryptography's Impact on Society: How Diffie and Hellman Changed the World. ACM, 2022. (ACM book honoring Turing Award winners Whitfield Diffie and Martin Hellman, edited by Rebecca Slayton).
9. S. Jiang, K. Khoo, C.Y. Lam, A.J. Menezes, P.C. van Oorschot. Chapter 15: Cryptography. K.H. Rosen, D.R. Shier and W. Goddard (editors), *Handbook of Discrete and Combinatorial Mathematics*, second edition (2017), 15:1-15:66.
10. A.J. Menezes, P.C. van Oorschot. Coding Theory and Cryptology, Chapter 14 (pp.889-954) in *Handbook of Discrete and Combinatorial Mathematics*, Kenneth H. Rosen (ed.), CRC Press 2000.
11. P.C. van Oorschot. A comparison of practical public-key cryptosystems based on integer factorization and discrete logarithms, Chapter 5 (pp.289-322) in *Contemporary Cryptology: The Science of Information Integrity*, G.J. Simmons (ed.), IEEE Press (1992).

12. I.F. Blake, P.C. van Oorschot, S.A. Vanstone. Complexity issues for public-key cryptography, pp.75-97 in *Performance Limits in Communication Theory and Practice*, J.K. Skwirzynski (ed.), Kluwer Academic Publishers 1988.

**Refereed journals (published papers, including accepted/to appear, where noted):**

13. Xavier de Carnavalet, P.C. van Oorschot. A survey and analysis of TLS interception mechanisms and motivations. *ACM Computing Surveys* (to appear; accepted Dec.12, 2022).
14. D. Barrera, C. Bellman, P.C. van Oorschot. Security best practices: A critical anlaysis using IoT as a case study. *ACM Transactions on Privacy and Security* 26(2) 13:1-13:30, March 2023.
15. C. Bellman, P.C. van Oorschot. Systematic analysis and comparison of security advice as datasets. *Computers & Security* vol.124 (Jan 2023), 102989-103000.
16. F. Alaca, P.C. van Oorschot. Comparative Analysis and Framework Evaluating Web Single Sign-On Systems, *ACM Computing Surveys*. 53(5) 112:1-112:34, Sept 2020.
17. F. Alaca, A. Abdou, P.C. van Oorschot. Comparative Analysis and Framework Evaluating Mimicry-Resistant and Invisible Web Authentication Schemes. *IEEE TDSC* 18(2):534-549, Mar-Apr 2021.
18. A. Abdou, P.C. van Oorschot, T. Wan. Comparative Analysis of Control Plane Security of SDN and Conventional Networks. *IEEE Comm. Surveys and Tutorials* 20(4):3542-3559, 4qtr2018.
19. C. Herley, P.C. van Oorschot. Science of Security: Combining Theory and Measurement to Reflect the Observable. *IEEE Security & Privacy* 16(1):2-12, Jan/Feb 2018. **Feature article** in special issue.
20. A. Abdou, A. Matrawy, P.C. van Oorschot. Server Location Verification (SLV) and Server Location Pinning: Augmenting TLS Authentication. *ACM Trans. Privacy & Security* 21(1), 1:1-1:26, Dec. 2017.
21. M.Mohamed, S.Gao, N.Sachdeva, N.Saxena, C.Zhang, P.Kumaraguru, P.C.van Oorschot. On security and usability of dynamic cognitive game CAPTCHAs. J. Computer Security 25(3): 205-230 (2017).
22. A.Abdou, A.Matrawy, P.C. van Oorschot. Location verification of wireless Internet clients: evaluations and improvements. *IEEE Trans. Emerging Topics in Computing* 5(4):563-575, Oct-Dec 2017.
23. A. Abdou, A. Matrawy, P.C. van Oorschot. CPV: Delay-based Location Verification for the Internet. *IEEE Trans. Dependable and Secure Computing* 14(2):130-144 (March-April, 2017).
24. D. Florencio, C. Herley, P.C. van Oorschot. Pushing on string: the don't-care region of password strength. *Communications of the ACM* 59(11):66-74 (November 2016).
25. J. Bonneau, C. Herley, P.C. van Oorschot, F. Stajano. Passwords and the Evolution of Imperfect Authentication. *Communications of the ACM* 58(7):78-87 (July 2015).
26. S. Chiasson, P.C. van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography* 77(2):401-408. Springer. 2015.
27. A. Abdou, A. Matrawy, P.C. van Oorschot. Accurate one-way delay estimation with reduced client-trustworthiness. *IEEE Communications Letters* 19(5):735-738 (May 2015).
28. A. Abdou, A. Matrawy, P.C. van Oorschot. Taxing the queue: hindering middleboxes from unauthorized large-scale traffic relaying. *IEEE Commn. Letters* 19(1):42-45 (Jan.2015).
29. C.Amrutkar, P.Traynor, P.C.van Oorschot. An empirical evaluation of security indicators in mobile web browsers. DOI: 10.1109/TMC.2013.90. *IEEE Trans. Mobile Computing* 14(5):889-903 (May 2015).
30. Yi Xu, Gerardo Reynaga, Sonia Chiasson, Jan-Michael Frahm, Fabian Monrose, Paul C. van Oorschot. Security Analysis and Related Usability of Motion-based CAPTCHAs: Decoding Codewords in Motion. *IEEE Trans. on Dependable and Secure Computing* 11(5):480-493 (Sept/Oct 2014).
31. M. Alsaleh, P.C. van Oorschot. Evaluation in the absence of absolute ground truth: toward reliable evaluation methodology for scan detectors. *Int. J. Information Security* 12(2):97-110, 2013.
32. R. Biddle, S. Chiasson, P.C. van Oorschot. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys* 44(4), Article 19:1-41 (August 2012).

33. S. Chiasson, E. Stobert, A. Forget, R. Biddle, P.C. van Oorschot. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. IEEE TDSC 9(2):222-235 (March/April 2012).
34. C. Herley, P.C. van Oorschot. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy* 10(1):28-36 (Jan/Feb 2012).
35. M. Alsaleh, M. Mannan, P.C. van Oorschot. Revisiting Defenses Against Large-Scale Online Password Guessing Attacks. *IEEE Trans. Dependable & Secure Computing* 9(1):128-141, 2012.
36. P.C. van Oorschot, G. Wurster. Reducing Unauthorized Modification of Digital Objects. *IEEE Transactions on Software Engineering* 38(1):191-204 (Jan/Feb.2012).
37. M. Alsaleh, P.van Oorschot. Revisiting Network Scanning Detection Using Sequential Hypothesis Testing. *Security & Communication Networks* 5(12):1337-1350 (2012), Wiley & Sons.
38. R. Biddle, M. Mannan, P.van Oorschot, T.Whalen. User Study, Analysis, and Usable Security of Passwords Based on Digital Objects. *IEEE Trans. Info. Forensics & Security* 6(3):970-979, 2011.
39. T. Jaeger, P.C. van Oorschot, G. Wurster. Countering Unauthorized Code Execution on Commodity Kernels: A Survey of Common Interfaces Allowing Kernel Code Modification. *Computers & Security* 30(8): 571-579 (2011).
40. P.C. van Oorschot, J. Thorpe. Exploiting Predictability in Click-Based Graphical Passwords. *Journal of Computer Security* 19(4): 669-702 (2011).
41. M. Mannan, P.C. van Oorschot. Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers. *Journal of Computer Security* 19(4): 703-750 (2011).
42. D. Barrera, P.C. van Oorschot. Secure Software Installation on Smartphones. *IEEE Security & Privacy* 9(3):42-48 (May/June 2011).
43. David Barrera, P.C. van Oorschot. Accommodating IPv6 Addresses in Security Visualization Tools. *Information Visualization* 10(2): 107-116 (April 2011).
44. P.C. van Oorschot, A. Salehi-Abari, J. Thorpe. Purely Automated Attacks on PassPoints-Style Graphical Passwords. *IEEE Trans. Information Forensics and Security* 5(3): 393-405, Sept.2010.
45. S.Chiasson, A.Forget, R.Biddle, P.C.van Oorschot. User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords. *Int'l J. Info. Security* 8(6):387-398, Dec.2009 (Springer).
46. J.A. Muir, P.C. van Oorschot. Internet Geolocation: Evasion and Counter-evasion. *ACM Computing Surveys* 42(1), Article 4:1-23 (Dec.2009).
47. M. Mannan, P.C. van Oorschot. Reducing Threats from Flawed Security APIs: The Banking PIN Case. *Computers & Security* 28(6): 410-420 (Sept.2009).
48. P.C. van Oorschot, J. Thorpe. On predictive models and user-drawn graphical password schemes. *ACM Transactions on Information and System Security* 10(4), article 17 pp.1-33 (Jan. 2008).
49. P.C. van Oorschot, T. Wan, E. Kranakis. On Inter-domain routing security and pretty secure BGP (psBGP), *ACM Trans. Information and System Security* 10(3), article 11 pp.1-41 (July 2007).
50. P.C. van Oorschot, S. Stubblebine. On countering online dictionary attacks with login histories and humans-in-the-loop. *ACM Trans. Information and System Security* 9(3): 235-258 (2006).
51. P.C. van Oorschot, J.M. Robert, M. Vargas Martin. A monitoring system for detecting repeated packets with applications to computer worms. Springer, *Int'l J. Info. Security* 5(3): 186-199 (2006).
52. P.C.van Oorschot, A.Somayaji, G.Wurster. Hardware-assisted circumvention of self-hashing software tamper resistance. *IEEE Trans. Dep. & Secure Comp.* (2)2: 82-92 (2005). **Invited** (peer-reviewed).
53. M. Smith, P.C. van Oorschot, M. Willett. Cryptographic Information Recovery Using Key Recovery, *Computers & Security* 19(1): 21-27, Elsevier Advanced Technology 2000.
54. P.C. van Oorschot, M.J. Wiener. Parallel collision search with cryptanalytic applications. *Journal of Cryptology* 12(1): 1-28 (Jan. 1999).

55. B. Preneel, P.C. van Oorschot. On the security of iterated message authentication codes. *IEEE Transactions on Information Theory* 45(1): 188-199 (Jan. 1999).
56. B. Preneel, V. Rijmen, P.C. van Oorschot. Security analysis of the Message Authenticator Algorithm (MAA), *European Trans. on Telecommunications* 8(5): 455-470 (Sept./Oct. 1997).
57. B. Preneel, P.C. van Oorschot. A key recovery attack on the ANSI X9.9 retail MAC, *Electronics Letters* 32(17): 1568-1569 (Aug.16 1996).
58. R. Rueppel, P.C. van Oorschot. Modern key agreement techniques, *Computer Communications* 17(7): 458-465 (July 1994).
59. W. Diffie, P.C. van Oorschot, M.J. Wiener. Authentication and authenticated key exchanges, *Designs, Codes and Cryptography* 2(2): 107-125 (1992).
60. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Subgroup refinement algorithms for root finding in GF(q), *SIAM Journal on Computing* 21(2): 228-239 (1992).
61. A. Beutelspacher, D. Jungnickel, P.C. van Oorschot, S.A. Vanstone. Pair-splitting sets in AG(m,q), *SIAM Journal on Discrete Mathematics* 5(4): 451-459 (Nov.1992).
62. P.C. van Oorschot, S.A. Vanstone. On splitting sets in block designs and finding roots of polynomials, *Discrete Mathematics* 84(1): 71-85 (1990).
63. C.J. Colbourn, P.C. van Oorschot. Applications of combinatorial designs in computer science, *ACM Computing Surveys* 21(2): 223-250 (Jun. 1989).
64. P.C. van Oorschot, S.A. Vanstone. A geometric approach to root finding in GF($q^m$), *IEEE Trans. on Information Theory* 35(2): 444-453 (Mar. 1989).

**Refereed journal articles, under submission (pending decision or revision):**

65. D. Barrera, C. Bellman, P.C. van Oorschot. A close look at a systematic method for analyzing sets of security advice. Submitted Aug 2022 to *Journal of Cybersecurity* (under revision).
66. J. Clark, P.C. van Oorschot, S. Ruoti, K. Seamons, D. Zappala. A Survey of Secure Email Systems and Stakeholders. Submitted Oct 2021 to *ACM Computing Surveys* (under revision).
67. P.C. van Oorschot, S. Stubblebine. On identity-theft and a countermeasure based on digital uniqueness and location cross-checking. Submitted Dec.2005 to *ACM Trans. Internet Technology* (conditionally accepted). Technical Report: TR-05-12 (Dec.2005), School of Computer Science, Carleton University.

**Conference proceedings papers, refereed:** (AR = acceptance rate)

68. F. Hao, P.C. van Oorschot. SoK: Password-authenticated key exchange – Theory, practice, standardization and real-world lessons. AsiaCCS 2022.
69. Srivathsan G. Morkonda, P.C. van Oorschot, S. Chiasson. Empirical analysis and privacy implications in OAuth-based single sign-on systems. WPES 2021.
70. J. Clark, P.C. van Oorschot, S. Ruoti, K. Seamons, D. Zappala. SoK: Securing Email—A Stakeholder-based Approach. Financial Cryptography 2021. Earlier version: arXiv.1804.07706 e-print, Cornell University Library, 19 pages, 20 Apr 2018.
71. S. Matsumoto, J. Bosamiya, Y. Dai, P.C. van Oorschot, B. Parno. CAPS: Smoothly transitioning to a more resilient web PKI. ACSAC 2020, 655-668.
72. C. Bennett, A. Abdou, P.C. van Oorschot. Empirical Scanning Analysis of Censys and Shodan. MAD Web 2021 (NDSS workshop on) Measurements, Attacks, and Defenses for the Web.
73. Hemant Gupta, P.C. van Oorschot. Onboarding and Software Update Architecture for IoT Devices. International Conference on Privacy, Security and Trust (PST 2019). 11 pages. **Best Paper award**.
74. C. Bellman, P.C. van Oorschot. Analysis, Implications and Challenges of an Evolving Consumer IoT Security Landscape. International Conference on Privacy, Security and Trust (PST 2019). 7 pages.

75. T. Murray, P.C. van Oorschot. Formal Proofs, the Fine Print and Side Effects. **Best Paper award**. SecDev 2018 (IEEE Cybersecurity Development Conf.), Sept.30-Oct.2, Cambridge, MA.
76. C. Herley, P.C. van Oorschot. Science, Security, and the Elusive Goal of Security as a Scientific Pursuit. May 2017 IEEE Symposium on Security and Privacy, pp.99-120. AR: 13.3%
77. A. Abdou, A. Matrawy, P.C. van Oorschot. Accurate Manipulation of Delay-based Internet Geolocation. **Distinguished Paper Award**. AsiaCCS'17, Abu Dhabi, UAE, April 2017, pp.887-898. AR: 20.3%
78. F. Alaca, P.C. van Oorschot. Device Fingerprinting for Augmenting Web Authentication: Classification and Analysis of Methods. ACSAC 2016, Dec.5-9 L.A., CA pp.289-301. AR: 22.8%
79. L. Zhang-Kennedy, S. Chiasson, P.C. van Oorschot. Revisiting password rules: Facilitating human management of passwords. APWG 2016 eCrime conference, pp.81-90. June 2016.
80. A. Abdou, D. Barrera, P.van Oorschot. What lies beneath? Analyzing automated SSH bruteforce attacks. Passwords 2015, pp.72-91, Springer LNCS v.9551. Cambridge UK, Dec 2015. AR: 33%
81. G. Reynaga, S. Chiasson, P.C. van Oorschot. Heuristics for the evaluation of CAPTCHAs on smartphones. Proc. of British HCI 2015, pp.126-135, July 13-17, Lincoln, U.K.
82. G. Reynaga, S. Chiasson, P.C. van Oorschot. Exploring the Usability of CAPTCHAs on Smartphones: Comparisons and Recommendations. DOI: 10.14722/usec.2015.23006. Proceedings of USEC'15, 8 February 2015, San Diego. 10 pages.
83. D. Florencio, C. Herley, P.C. van Oorschot. An Administrator's Guide to Internet Password Research. Proc. USENIX LISA 2014, pp.35-52, Nov.9-14, Seattle, Washington. AR: 31%
84. A. Abdou, A. Matrawy, P.C. van Oorschot. Location Verification on the Internet: Towards Enforcing Location-aware Access Policies Over Internet Clients. IEEE CNS 2014, pp.175-183, Oct.29-31, San Francisco. AR: 29%
85. D. Florencio, C. Herley, P.C. van Oorschot. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. USENIX Security 2014, pp.575-590, Aug.20-22, San Diego, California. AR: 19%
86. D. Barrera, D. McCarney, J. Clark, P.C. van Oorschot. Baton: Certificate Agility for Android's Decentralized Signing Infrastructure. WiSec 2014, pp.1-12, July 22-24, Oxford, U.K. AR: 26%
87. Manar Mohamed, Niharika Sachdeva, Michael Georgescu, Song Gao, Nitesh Saxena, Chengcui Zhang, Ponnurangam Kumaraguru, P.C. van Oorschot, Wei-Bang Chen. A Three-Way Investigation of a Game-CAPTCHA: Automated Attacks, Relay Attacks and Usability. ACM ASIACCS 2014, June 4-6, Kyoto, Japan, pp.195-206. AR: 20%
88. A. Skillen, D. Barrera, P.C. van Oorschot. Deadbolt: Locking Down Android Disk Encryption (full paper). ACM SPSM 2013 (Security and Privacy in Smartphones and Mobile Devices), pp.3-14, November 2013, Berlin. AR: 24% (1 of 5 full papers accepted along with 8 short papers from 54 total submissions).
89. J. Clark, P.C. van Oorschot. SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. IEEE Symp. Security and Privacy, pp.511-525, May 2013. AR: 12%
90. D. McCarney, D. Barrera, J. Clark, S. Chiasson, P.C. van Oorschot. Tapas: Design, Implementation, and Usability of a Password Manager. ACSAC 2012, pp.89-98 . AR: 19%
91. D. Barrera, J. Clark, D. McCarney, P.C. van Oorschot. Understanding and Improving App Installation Security Mechanisms through Empirical Analysis of Android. 2nd ACM CCS Workshop on Security & Privacy in Mobile Devices (SPSM), pp.81-92, Oct.2012. AR: 36.7%. Earlier Tech. Rpt TR-12-01 (May 7 2012), School of Comp. Sci., Carleton U.
92. Chaitrali Amrutkar, Patrick Traynor, P.C. van Oorschot. Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road? **Best Student Paper**. ISC 2012: Information Security Conference, pp.86-103. Germany. AR: 32%

93. Yi Xu, G. Reynaga, S. Chiasson, Jan-Michael Frahm, F. Monrose, P.C. van Oorschot. Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion. USENIX Security, pp.49-64, Aug.2012. AR: 19.4%
94. J. Bonneau, C. Herley, P.C. van Oorschot, F. Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Symp. Security & Privacy, May 2012, pp.553-567. AR: 13%. Full version (32 pages): University of Cambridge Computer Lab, Tech. Rpt No. 817 (UCAM-CL-TR-817), March 2012.
95. D. Barrera, W. Enck, P.C. van Oorschot. Meteor: Seeding a Security-Enhancing Infrastructure for Multi-market Application Ecosystems. IEEE MoST 2012 (Mobile Security Technologies workshop), San Francisco, May 2012. 10 pages. AR: 39.3%. Updates and obsoletes technical report: Seeding a Security-Enhancing Infrastructure for Multi-market Application Ecosystems, TR-11-06 (Apr.22, 2011), Carleton University, School of Computer Science.
96. K. Bicakci, P.C. van Oorschot. A Multi-Word Password Proposal (gridWord) and Exploring Questions about Science in Security Research and Usable Security Evaluation. Proc. NSPW 2011, pp.25-36 (ACM) Sept.12-15, Marin County, CA. AR: 37.5%.
97. M. Alsaleh, P.C. van Oorschot. Network Scan Detection with LQS: A Lightweight, Quick and Stateful Algorithm. ASIACCS 2011, pp.102-113. AR: not known.
98. K. Bicakci, N.B. Atalay, M. Yuceel, P.C. van Oorschot. Exploration and Field Study of a Browser-based Password Manager using Icon-based Passwords. 2nd Workshop on Real-Life Cryptographic Protocols and Standardization (RLCPS'11), 4 March 2011, St. Lucia (FC 2011 workshop). Springer (2012) LNCS 7126, pp.104-118. AR: not known.
99. M. Mannan, D. Barrera, C. Brown, D. Lie, P.C. van Oorschot. Mercury: Recovering Forgotten Passwords Using Personal Devices. Springer LNCS 7035 pp.315-330 (Springer, 2012), Financial Crypto and Data Security (FC 2011).
100. E. Stobert, A. Forget, S. Chiasson, P.C. van Oorschot, R. Biddle. Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords. ACSAC 2010. (AR: 17.2%)
101. D. Barrera, H.G. Kayacik, P.C. van Oorschot, A. Somayaji. A Methodology for Empirical Analysis of Permission-Based Security Models and Its Application to Android. ACM CCS 2010. (AR: 17.2%)
102. G. Wurster, P.C. van Oorschot. A Control Point for Reducing Root Abuse of File-System Privileges. ACM CCS 2010. (AR: 17.2%)
103. R. Biddle, P.C. van Oorschot, A.S. Patrick, J. Sobey, T. Whalen. Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study. CCSW 2009: The ACM Cloud Computing Security Workshop (in conjunction with ACM CCS 2009), Chicago. (AR: unknown)
104. S. Chiasson, A. Forget, E. Stobert, P.C. van Oorschot, R. Biddle. Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords. ACM CCS 2009, Chicago. (AR: 18.4%)
105. D. Barrera, P. van Oorschot. Security Visualization Tools and Source Addresses in IPv6. VizSec 2009: Workshop on Visualization for Cyber Security. Oct.11, 2009, Atlantic City, NJ. (AR: 43%)
106. Glenn Wurster, P.C. van Oorschot. System Configuration as a Privilege. USENIX Hot Topics in Security 2009, Montreal. (AR: 28%)
107. P.C. van Oorschot, T. Wan. TwoStep: An Authentication Method Combining Text and Graphical Passwords. MCETECH 2009: 4th International MCETECH Conference on eTechnologies, 4-6 May 2009, Ottawa. Springer LNBIP vol.26, pp.233-239. (AR: unknown)
108. M. Alsaleh, D. Barrera, P.C. van Oorschot. Improving Security Visualization with Exposure Map Filtering. 24th ACSAC, Dec.8-12, 2008, Anaheim, California. (AR: 24%)
109. A. Salehi-Abari, J. Thorpe, P.C. van Oorschot. On Purely Automated Attacks and Click-Based Graphical Passwords. 24th ACSAC, Dec.8-12, 2008, Anaheim, California. (AR: 24%)

110. T. Oda, G. Wurster, P.C. van Oorschot, A. Somayaji. SOMA: Mutual Approval for Included Content in Web Pages. ACM CCS 2008, Oct.27-31 2008, Alexandria, VA, USA. (AR: 18.1%)
111. J. Sobey, R. Biddle, P.C. van Oorschot, A.S. Patrick. Exploring User Reactions to Browser Cues for Extended Validation Certificates. European Symp. Research in Computer Security (ESORICS 2008), Malaga, Spain. (AR: 22%)
112. D. Nali, P.C. van Oorschot. CROO: A Universal Infrastructure and Protocol to Detect Identity Fraud. European Symp. Research in Computer Security (ESORICS 2008), Malaga. (AR: 22%)
113. G. Wurster, P.C. van Oorschot. The Developer is the Enemy. NSPW 2008 - New Security Paradigms Workshop. September 2008, Olympic Valley, California. (AR: 30.6%)
114. M. Mannan, P.C. van Oorschot. Localization of Credential Information to Address Increasingly Inevitable Data Breaches. New Security Paradigms Workshop 2008, Olympic Valley, CA. (AR: 30.6%)
115. S. Chiasson, A. Forget, R. Biddle, P. van Oorschot. Influencing Users Towards Better Passwords: Persuasive Cued Click-Points. HCI 2008, Sept, Liverpool, UK (AR: 28% of full papers)
116. M. Mannan, P.C. van Oorschot. Digital Objects as Passwords. USENIX Hot Topics in Security 2008, San Jose, California. (AR: 32.4%)
117. A. Forget, S. Chiasson, P.C. van Oorschot, R. Biddle. Improving Text Passwords Through Persuasion. SOUPS 2008 (Symposium on Usable Privacy and Security), July 23-25 2008, Pittsburgh, PA. (AR: 27.9%)
118. A. Forget, S. Chiasson, P.C. van Oorschot, R. Biddle. Persuasion for Stronger Passwords: Motivation and Pilot Study. Third International Conference on Persuasive Technology, Oulu, Finland (June 2-4 2008). Springer LNCS vol.5033/2008, pp.140-150. (AR: 45% of full papers)
119. A. Hijazi, H. Inoue, A. Matrawy, P.C. van Oorschot, A. Somayaji. Discovering Packet Structure through Lightweight Hierarchical Clustering. ICC 2008, Beijing, China, May 2008. (AR: 36%)
120. M. Mannan, P.C. van Oorschot. Privacy-Enhanced Sharing of Personal Content on the Web. World Wide Web Conference: WWW 2008, April 21-25. Beijing, China. (AR: 11%)
121. S. Chiasson, J. Srinivasan, R. Biddle, P. van Oorschot. Centered Discretization with Application to Graphical Passwords. USENIX UPSEC 2008 (Usability, Psychology & Security), Apr.14 2008, SFO. (AR: 26.6% of full papers)
122. M. Mannan, P.C. van Oorschot. Weighing Down The Unbearable Lightness of PIN Cracking. Financial Cryptography and Data Security (FC 2008), Cozumel, Mexico, pp.176-181 in Springer LNCS vol.5143. (AR: 30%)
123. D. Whyte, P.C. van Oorschot, E. Kranakis. Tracking Darkports for Network Defense. **Outstanding Paper Award**. ACSAC 2007, Miami Beach, Florida. (AR: 22%)
124. S. Chiasson, P.C. van Oorschot, R. Biddle. Graphical Password Authentication Using Cued Click Points. ESORICS 2007, Dresden, Germany. Springer LNCS 4734 (2007), pp.359-374. (AR: 23.8%)
125. M. Mannan, P.C. van Oorschot. Security and Usability: The Gap in Real-World Online Banking. New Security Paradigms Workshop (NSPW 2007), New Hampshire, USA. (AR: 38%)
126. D. Nali, P.C. van Oorschot, A. Adler. VideoTicket: Detecting Identity Fraud Attempts via Audiovisual Certificates and Signatures. New Security Paradigms (NSPW 2007), New Hampshire. (AR: 38%)
127. J. Thorpe, P.C. van Oorschot. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. 16th USENIX Security Symposium, Aug.6-10 2007, Boston, MA. (AR: 12.3%)
128. G. Wurster, P.C. van Oorschot. Self-signed Executables: Restricting Replacement of Program Binaries by Malware. USENIX Hot Topics in Security 2007, Boston, USA. (AR: 33%)
129. S. Chiasson, Robert Biddle, P.C. van Oorschot. A Second Look at the Usability of Click-Based Graphical Passwords. **Best Paper Award**. Symposium on Usable Privacy and Security, SOUPS 2007. (AR: 31.7%)

130. J. Clark, P.C. van Oorschot, C. Adams. Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability. Symposium on Usable Privacy and Security: SOUPS 2007. (AR: 31.7%)
131. M. Mannan, P.C. van Oorschot. Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer. Financial Crypto & Data Security (FC'07), Trinidad and Tobago, 2007. (AR: 20%)
132. D. Whyte, P.C. van Oorschot, E. Kranakis. Addressing SMTP-based Mass-Mailing Activity Within Enterprise Networks. ACSAC 2006, Miami Beach, Florida. (AR: 30.3%)
133. S. Chiasson, P.C. van Oorschot, R. Biddle. A Usability Study and Critique of Two Password Managers. USENIX Security 2006, Aug.2-4, Vancouver. (AR: 12.3%)
134. D. Whyte, P.C. van Oorschot, E. Kranakis. Exposure Maps: Removing Reliance on Attribution During Scan Detection. USENIX Hot Topics in Security 2006, Vancouver, Canada. (AR: 19.6%)
135. Tao Wan, P.C. van Oorschot. Analysis of BGP Prefix Origins During Google's May 2005 Outage. Proc. 2nd International Workshop on Security in Systems and Networks (SSN2006), Rhode Island, Greece, Apr.25 2006 (in conjunction with IEEE IPDPS). (AR: unknown)
136. M. Mannan, P.C. van Oorschot. A Protocol for Secure Public Instant Messaging. Financial Cryptography and Data Security (FC'06), Feb.27-Mar.2 2006, Anguilla, British West Indies, pp.20-35, Springer LNCS vol.4107/2006. (AR: 39% of full papers)
137. D. Whyte, P.C. van Oorschot, E. Kranakis. Detecting Intra-Enterprise Scanning Worms Based on Address Resolution. 21st Annual Computer Security Applications Conf. (ACSAC), Dec. 5-9, 2005, Tucson, AZ (IEEE Computer Society). (AR: 22.5%)
138. M. Mannan, P.C. van Oorschot. Instant Messaging Worms, Analysis and Countermeasures. WORM 2005 (ACM Workshop on Rapid Malcode), Nov. 2005, Fairfax, Virginia. (AR: 25%)
139. P.C. van Oorschot. Message Authentication by Integrity with Public Corroboration. ACSA 2005 New Security Paradigms Workshop, Sept. 2005, Lake Arrowhead, CA (ACM ). (AR: 28.6%)
140. J. Thorpe, P.C. van Oorschot, A. Somayaji. Pass-Thoughts: Authenticating With Our Minds. ACSA New Security Paradigms Workshop, Lake Arrowhead, CA, USA, Sept. 2005 (ACM). (AR: 28.6%)
141. A. Matrawy, P.C. van Oorschot, A. Somayaji. Mitigating Network Denial of Service through Diversity-Based Traffic Management. Applied Cryptography and Network Security: 3rd International Conference, ACNS 2005, New York, June 7-10, 2005. Springer LNCS 3531, pp.104-121. (AR: 22%)
142. G. Wurster, P.C. van Oorschot, A. Somayaji. A Generic Attack on Checksumming-Based Software Tamper Resistance. pp.127-138 in: Proc. 2005 IEEE Symp. on Security and Privacy, Oakland, Cal., IEEE Computer Society. (AR: 8.9%)
143. P. C. van Oorschot, S. Stubblebine. Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling. Proc. of Financial Cryptography and Data Security 2005 (FC'05), Feb.28-Mar.3 2005, Commonwealth of Dominica. pp.31-43, Springer LNCS 3570. (AR: 24%)
144. T. Wan, E. Kranakis, P.C. van Oorschot. Pretty Secure BGP. Proc. Network and Distributed System Security (NDSS'05), Feb. 2005, San Diego (Internet Society). (AR: 13%)
145. D. Whyte, E. Kranakis, P.C. van Oorschot. DNS-based Detection of Scanning Worms in an Enterprise Network. Proc. Network and Dist. Sys. Security (NDSS'05), Feb.2005, San Diego (Internet Society). (AR: 13%)
146. J. Thorpe, P.C. van Oorschot. Towards Secure Design Choices for Implementing Graphical Passwords. pp.50-60 in: Proc. 20th Annual Computer Security Applications Conf. (ACSAC), Dec.2004, Tucson, AZ, IEEE Computer Society (2004). (AR: 26%)

147. T. Wan, E. Kranakis, P.C. van Oorschot. Securing the Destination Sequenced Distance Vector Routing Protocol (S-DSDV). Proc. ICICS'04 (6th International Conf. Info. and Comm, Security), Oct. 2004, Malaga, Spain. (Springer LNCS 3269, pp.358-374). (AR: 17%)
148. M. Mannan, P.C. van Oorschot. Secure Public Instant Messaging: A Survey. Proc. of Privacy, Security and Trust, proceedings, pp.69-77, Oct. 2004, Fredericton, NB. (AR: unknown)
149. J. Thorpe, P.C. van Oorschot. Graphical Dictionaries and the Memorable Space of Graphical Passwords. Proc. 13th USENIX Security 2004, pp.135-150, Aug. 2004, San Diego. (AR: 12%)
150. T. Wan, E. Kranakis, P.C. van Oorschot. S-RIP: A Secure Distance Vector Routing Protocol. Proc. ACNS'04 (academic track): 2nd International Conf. on Applied Cryptography and Network Security, Yellow Mountain, China, June 2004, pp.103-119, Springer LNCS 3089. (AR: 12%)
151. S. Stubblebine, P.C. van Oorschot. Addressing Online Dictionary Attacks with Login Histories and Humans-in-the-Loop (extended abstract). Proc. Financial Cryptography, 8th International Conf., FC 2004, Key West, Feb. 2004, pp.39-53, Springer LNCS 3110. (AR: 22%)
152. S.Chow, P.Eisen, H.Johnson, P. Van Oorschot. White-Box Cryptography and an AES Implementation. Proc. SAC 2002 - 9th Annual Workshop on Selected Areas in Cryptography, Aug. 15-16 2002, St. John's, Canada (pp.250-270, Springer LNCS 2595, 2003).
153. S.Chow, P.Eisen, H.Johnson, P. Van Oorschot. A White-Box DES Implementation for DRM Applications. Proc. 2nd ACM Workshop on Digital Rights Management (DRM 2002), ACM CCS-9 workshop, Nov. 18 2002, Washington D.C. (pp.1-15, Springer LNCS 2696, 2003).
154. M. Just, P.C. van Oorschot. Addressing the problem of undetected signature key compromise. Proc. Internet Society 1999 Symp. on Network and Distributed System Security (NDSS'99).
155. P.C. van Oorschot, M.J. Wiener. Improving meet-in-the-middle attacks by orders of magnitude, Crypto'96, Springer LNCS vol.1109, pp.229-236, 1996.
156. B. Preneel, P.C. van Oorschot. On the security of two MAC algorithms, Eurocrypt'96, Springer LNCS vol.1070, pp.19-32, 1996.
157. P.C. van Oorschot, M.J. Wiener. On Diffie-Hellman key agreement with short exponents. Eurocrypt'96, Springer LNCS vol.1070, pp.332-343, 1996.
158. B. Preneel, P.C. van Oorschot. MDx-MAC and building fast MACs from hash functions. Crypto'95, Springer LNCS vol.963, 1995.
159. P.C. van Oorschot, M.J. Wiener. Parallel collision search with applications to hash functions and discrete logarithms. pp.210-218, proceedings, 2nd ACM Conf. on Computer and Communications Security, Nov. 1994, Fairfax, Virginia.
160. M. Just, E. Kranakis, D. Krizanc, P.C. van Oorschot. On key distribution via true broadcasting. pp.81-88, proceedings, 2nd ACM Conference on Computer and Communications Security, Nov. 1994, Fairfax, Virginia.
161. P. Syverson, P.C. van Oorschot. On unifying some cryptographic protocol logics. pp.14-28, proceedings, 1994 IEEE Symp. on Research in Security & Privacy, 1994 May 16-18, Oakland, CA.
162. P.C. van Oorschot. An alternate explanation of two BAN-logic `failures', Eurocrypt'93, Springer LNCS vol.765, pp.443-447 (1994).
163. P.C. van Oorschot. Extending cryptographic logics of belief to key agreement protocols. pp.232-243, proceedings, 1st ACM Conference on Computer and Commns Security, Nov. 1993, Fairfax, Virginia.
164. P.C. van Oorschot. A comparison of practical public-key cryptosystems based on integer factorization and discrete logarithms (extended abstract). Crypto'90, Springer LNCS vol.537, pp.576-581 (1991).
165. P.C. van Oorschot, M.J. Wiener. A known-plaintext attack on two-key triple encryption. Eurocrypt'90, Springer LNCS 473, pp.318-325, 1991.

166. P.C. van Oorschot, S.A. Vanstone. Some geometric aspects of root finding in GF($q^m$), pp.303-307, Contemporary Math. vol.111 (Finite Geometries and Combinatorial Designs), E.S. Kramer and S.S. Magliveras (eds.), AMS 1990.
167. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Some computational aspects of root finding in GF($q^m$). pp.259-270, Symbolic and Algebraic Computation, Springer LNCS 358, 1989.

**Other publications (editorials, panels, other unrefereed articles):**

168. P.C. van Oorschot. Memory errors and memory safety: A look at Java and Rust. *IEEE Security & Privacy* 21(3), May-Jun 2023. Security Knowledge column.
169. P.C. van Oorschot. Memory errors and memory safety: C as a case study. *IEEE Security & Privacy* 21(2):70-76, Mar-Apr 2023. Security Knowledge column.
170. P.C. van Oorschot. Security as an artificial science, administration, and tools. *IEEE Security & Privacy* 20(6):74-78, Nov-Dec 2022. Security Knowledge column.
171. P.C. van Oorschot. Cyber security education: reinvention required. *Cyber Today* magazine (Australia), 2022 Edition 1, pages 41-45, Australian Information Security Association. https://cybertoday.partica.online/cyber-today/cyber-today-edition-1-2022/flipbook/1/
172. P.C. van Oorschot. A view of security as 20 subject areas in four themes. *IEEE Security & Privacy* 20(1):102-108, Jan-Feb 2022. Security Knowledge column.
173. P.C. van Oorschot. Co-evolution of security's body of knowledge and curricula. *IEEE Security & Privacy* 19(5):83-89, Sep-Oct 2021. Security Knowledge column.
174. P.C. van Oorschot. Towards Unseating the Unsafe C Programming Language. "From the Editors", *IEEE Security & Privacy* 19(2):4-6, Mar-Apr 2021.
175. P.C. van Oorschot. Blockchains and Stealth Tactics for Teaching Security. "From the Editors", *IEEE Security & Privacy* 18(5):3-5, Sep-Oct 2020.
176. P.C. van Oorschot. Untangling Security and Privacy. "From the Editors", *IEEE Security & Privacy* 18(2):4-6, Mar-Apr 2020.
177. P.C. van Oorschot, Sean W. Smith. The Internet of Things: Security Challenges. Guest Editor's Introduction, Special Issue (The IoT and Security and Privacy), *IEEE Security & Privacy* 17(5):7-9, Sept-Oct 2019.
178. P.C. van Oorschot. Software Security and Systematizing Knowledge. "From the Editors", *IEEE Security & Privacy* 17(3):4-6, May-June 2019.
179. Kevin R.B. Butler, Robert K. Cunningham, P.C. van Oorschot, Reihaneh Safavi-Naini, A. Matrawy, Jeremy Clark. A Discussion on Security Education in Academia (panel). ACM CCS 2018, 2187-2188.
180. P.C. van Oorschot. Internet of Things Security: Is Anything New?. "From the Editors", *IEEE Security & Privacy* 16(5):4-6, Sept-Oct 2018.
181. John D. McLean, Cormac Herley, P.C. van Oorschot. On the Science of Security (McLean); Response (Herley, van Oorschot). Letter to the Editor. *IEEE Security & Privacy* 16(3):6-10, May-Jun 2018.
182. P.C. van Oorschot. Science, Security and Academic Literature: Can We Learn from History? (Invited). 2 pages. 2017 ACM CCS Moving Target Defense Workshop (MTD'17).
183. A. Abdou, P.C. van Oorschot. Secure Client and Server Geolocation over the Internet. *;login:* (The USENIX Magazine), 43(1):19-25 (Spring 2018). [edited; not peer-reviewed].
184. S. Egelman, C. Herley, P.C. van Oorschot. Markets for Zero-Day Exploits: Ethics and Implications. Panel note. New Security Paradigms Workshop 2013 (NSPW), pp.41-46, Banff, Canada. [at invitation of program committee]

185. M. Mannan, P.C. van Oorschot. Passwords for Both Mobile and Desktop Computers: ObPwd for Firefox and Android. *;login:* (The USENIX Magazine), 37(4):28-37 (Aug 2012). [edited; not peer-reviewed].
186. Dirk Balfanz, Richard Chow, Ori Eisen, M. Jakobsson, Steve Kirsch, Scott Matsumoto, J. Molina, Paul van Oorschot. The Future of Authentication. *IEEE Security & Privacy* 10(1):22-27 (Jan/Feb 2012) [edited; not peer-reviewed].
187. D. Barrera, G. Wurster, P.C. van Oorschot. Back to the Future: Revisiting IPv6 Privacy Extensions. *;login:* (The USENIX Magazine), 36(1), Feb.2011 [edited; not peer-reviewed].
188. P.C. van Oorschot. System Security, Platform Security and Usability (extended abstract, 2 pages). Invited. Proc. 5th ACM Workshop on Scalable Trusted Computing (ACM STC'10), 4 Oct 2010, Chicago. [invited; not peer-reviewed].
189. C. Herley, P.C. van Oorschot, A.S. Patrick. Passwords: If We're So Smart, Why Are We Still Using Them? Financial Crypto & Data Security (FC 2009), Barbados. Springer LNCS 5628/2009, p.230-237. [invited; not peer-reviewed].
190. T. Wan, P.C. van Oorschot, E. Kranakis. A Selective Introduction to Border Gateway Protocol (BGP) Security Issues. Proc. of NATO Advanced Studies Institute on Network Security and Intrusion Detection, Nork, Yerevan, Armenia, Oct.1-12 2005, IOS Press (2006). Tech. Report version: TR-05-07 (August 2005), School of Computer Science, Carleton Univ.
191. A. Main, P.C. van Oorschot. Software Protection and Application Security: Understanding the Battleground. Int. Course on State of the Art and Evolution of Computer Security and Industrial Cryptography, Heverlee, Belgium, June 2003. Proceedings: Springer LNCS (to appear).
192. P.C. van Oorschot. Revisiting Software Protection (invited paper). Proc. of 6th International Info. Security Conference (ISC 2003), Bristol, UK, Oct 2003, Springer LNCS 2851, pp.1-13.
193. P.C. van Oorschot. Design Choices and Security Implications in Implementing Diffie-Hellman Key Agreement (invited). Cryptography and Coding, Proceedings of 5th IMA Conference, Cirencester, UK, Dec.18-20 1995. Springer LNCS 1025/1995, page 1.
194. B. Preneel, P.C. van Oorschot. Further comments on keyed MD5. *CryptoBytes* 1(3): page 15 (summer 1995). RSA Laboratories technical newsletter.
195. P.van Oorschot. Security in GSM, *Telesis*, Issue No. 94 (Jul 1992), pp.58-60, Northern Telecom.

**Technical reports and manuscripts (not peer reviewed):**

196. Markus Miettinen, P.C.van Oorschot, Ahmad-Reza Sadeghi. Baseline functionality for security and control of commodity IoT devices and domain-controlled device lifecycle management. eprint: arXiv:1808.03071 (version: 9 Aug 2018).
197. J. Sobey, P.C. van Oorschot, A.S. Patrick. Browser Interfaces and EV-SSL Certificates: Confusion, Inconsistencies and HCI Challenges. Technical Report TR-09-02 (Jan.2009), School of Computer Science, Carleton University.
198. A. Hijazi, H. Inoue, A. Matrawy, P.C. van Oorschot, A. Somayaji. Lightweight Hierarchical Clustering of Network Packets using (p,n) grams. Technical Report TR-09-03 (Feb.2009), School of Computer Science, Carleton University.
199. D. Nali, P.C. van Oorschot. Simple Blind Search on Public-Key Encrypted Data. Technical Report TR-07-14 (May 2007), School of Computer Science, Carleton University.
200. D. Whyte, P.C. van Oorschot, E. Kranakis. Tracking Darkports for Network Defense. Extended version of ACSAC 2007 paper. Technical Report TR-07-04 (Feb. 2007), School of Computer Science, Carleton University.

201. M. Mannan, P. van Oorschot. A Protocol for Secure Public Instant Messaging. Extension of FC 2006 paper. Tech Rpt TR-06-01 (Jan.2006), School of Computer Science, Carleton University.
202. P. Syverson, P. van Oorschot. A unified cryptographic protocol logic. Report 5540-227, Center for High Assurance Computer Systems, Naval Research Lab (NRL CHACS), USA, 1996.

**Issued Patents: (18 U.S., 2 Canadian)**

203. U.S.Patent 7,174,563, Computer network security system and method having unilateral enforceable security policy provision. Feb.6, 2007. M. Brownlie, S. Hillier, P. Van Oorschot.
204. U.S. Patent 7,010,582 B1, Systems and apparatus providing interactions between multiple servers and an end use device. Mar.7 2006. R. Cheng, P. Van Oorschot, S. Hillier.
205. U.S. Patent 6,694,434, Method and apparatus for controlling program execution and program distribution. Feb.17, 2004. W. McGee, G. Langford, P. Van Oorschot
206. U.S. Patent 6,567,914, Apparatus and method for reducing transmission bandwidth and storage requirements in a cryptographic security system. May 20, 2003. M. Just, P. Van Oorschot.
207. U.S. Patent 6,393,568, Encryption and decryption system and method with content analysis provision. May 21, 2002. M. Ranger, P. Van Oorschot.
208. U.S. Patent 6,370,249, Method and apparatus for public key management. April 9, 2002. P. Van Oorschot.
209. U.S. Patent 6,341,164, Method and apparatus for correcting improper encryption and/or for reducing memory storage. January 22, 2002. L. Dilkie, P. Van Oorschot.
210. U.S. Patent 6,317,829, Public key cryptography based security system to facilitate secure roaming of users. Nov.13 2001. P. Van Oorschot.
211. U.S. Patent 6,229,894, Method and apparatus for access to user-specific encryption information. May 8, 2001. P. Van Oorschot, T. Moses.
212. U.S. Patent 6,215,872, Method for creating communities of trust in a secure communication system. Apr.10 2001. P. Van Oorschot.
213. U.S. Patent 6,202,157, Computer network security system having unilateral enforceable security policy provision. Mar.13 2001. M. Brownlie, S. Hillier, P. Van Oorschot.
214. U.S. Patent 6,134,550, Method and apparatus for use in determining validity of a certificate in a communication system employing trusted paths. Oct 17 2000. P.Van Oorschot, M.Wiener, I.Curry
215. U.S. Patent 6,134,327, Method and apparatus for creating communities of trust in a secure communication system. Oct.17 2000. P. Van Oorschot.
216. U.S. Patent 6,128,740, Computer security system and method with on demand publishing of certificate revocation lists. Oct.3 2000. I. Curry, P. Van Oorschot.
217. U.S. Patent 6,092,201, Method and apparatus for extending secure communication operations via a shared list. July 18 2000. J. Turnbull, I. Curry, P. Van Oorschot, S. Hillier.
218. U.S. Patent 5,850,443, Key management system for mixed-trust environment. Dec.15, 1998. P. Van Oorschot, M. Wiener.
219. Canadian Patent 2,213,096, Key management system for mixed-trust environments, Oct.31 2000. P. Van Oorschot, M. Wiener.
220. U.S. Patent 5,699,431, Method for efficient management of certificate revocation lists and update info. Dec.16, 1997. P. Van Oorschot, W. Ford, S. Hillier, J. Otway.
221. U.S. Patent 5,664,016, Method of building fast MACs from hash functions. Sept.2, 1997. B. Preneel, P. Van Oorschot.
222. Canadian Patent 2,213,096, Key management system for mixed-trust environments, Oct 31 2000. P. Van Oorschot, M. Wiener.

# Lianying Zhao

Assistant Professor
School of Computer Science ⋄ Carleton University
1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada

Email : lianying.zhao@scs.carleton.ca


**Dated:** August 6, 2023

## Research Interests

Trusted computing; Hardware/architectural security; Systems security; Security metrics; Authentication and privacy

## Education

- **Ph.D. in Information Systems Engineering** July 2018
  *Concordia University, Montreal, QC, Canada*
  - Dissertation: Authentication and Data Protection under Strong Adversarial Model
  - Supervisor: Dr. Mohammad Mannan
- **M.Eng. in Communication and Information System** June 2007
  *Tianjin University, Tianjin, China*
- **B.Eng. in Electronic Information Engineering** June 2004
  *Tianjin University, Tianjin, China*

## Employment

- **Assistant Professor** July 2019 – Present
  *Carleton University, Ottawa, ON, Canada*
- **NSERC Post-Doctoral Research Fellow** September 2018 – June 2019
  *University of Toronto, Toronto, ON, Canada*
- **Staff Software Engineer** July 2007 – December 2012
  *International Business Machines (IBM China), Beijing, China*

## Research Support

- **NOVA - FRQNT-CRSNG pour chercheurs et chercheuses de la relève** CAD $75,000/year for 3 years plus Montant Équipement ($36,298, TBD), 2023. Portion as co-PI: $30,000/year
- **Natural Sciences and Engineering Research Council (NSERC) – Alliance Grant,** with Ericsson Canada, CAD $65,000/year for 3 years, 2021
- **Natural Sciences and Engineering Research Council (NSERC) – Discovery Grant (DG),** CAD $29,000/year for 5 years, 2020
- **Natural Sciences and Engineering Research Council (NSERC) – Discovery Launch Supplement,** CAD $12,500, 2020
- **Mitacs Accelerate (with Ericsson Canada),** CAD $65,000, 2020
- **Carleton University Start-up Grant,** CAD $63,500, 2019
- **Natural Sciences and Engineering Research Council (NSERC) – Postdoctoral Fellowship (PDF),** CAD $90,000, 2018
- **Concordia University Full Tuition Award,** valued ∼CAD $39,000, 2013

## Publications

- **Refereed Conference/Workshop Publications**
  - Supraja Baskaran, **Lianying Zhao**, Mohammad Mannan, Amr Youssef. Measuring the Leakage and Exploitability of Authentication Secrets in Super-apps: The WeChat Case. *Symposium on Research in Attacks, Intrusions and Defenses (RAID'23)*, Oct. 16-18, 2023, Hong Kong (To appear).
  - Siqi Zhang, Mengyuan Zhang, **Lianying Zhao**. VIET: A Tool for Extracting Essential Information from Vulnerability Descriptions for CVSS Evaluation. *IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'23)*, Jul. 19-21, 2023, Sophia Antipolis, France.
  - He Shuang, **Lianying Zhao**, David Lie. vWitness: Certifying Web Page Interactions with Computer Vision. *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'23)*, Jun. 27-30, 2023, Porto, Portugal.
  - Ming Lei, **Lianying Zhao**, Makan Pourzandi, Fereydoun Farrahi Moghaddam. A Hybrid Decision-making Approach to Security Metrics Aggregation in Cloud Environments. *IEEE International Conference on Cloud Computing Technology and Science (CloudCom'22)*, Dec. 13-16, 2022, Bangkok, Thailand.
  - **Lianying Zhao**, Muhammad Shafayat Oshman, Mengyuan Zhang, Fereydoun Farrahi Moghaddam, Shubham Chander, Makan Pourzandi. Towards 5G-ready Security Metrics. *IEEE International Conference on Communications (ICC'21)*, Jun. 14-23, 2021.
  - Rongzhen Cui, **Lianying Zhao**, David Lie. Emilia: Catching Iago in Legacy Code. *Network and Distributed System Security Symposium (NDSS'21)*, Feb. 21-25, 2021.
  - He Shuang, Wei Huang, Pushkar Bettadpur, **Lianying Zhao**, Ivan Pustogarov, David Lie. Using Inputs and Context to Verify User Intentions in Internet Services. *ACM SIGOPS Asia-Pacific Workshop on Systems (APSys'19)*, Aug. 19-20, 2019, Hangzhou, China.
  - **Lianying Zhao**, Mohammad Mannan. TEE-aided Write Protection Against Privileged Data Tampering. *Network and Distributed System Security Symposium (NDSS'19)*, Feb. 24-27, 2019, San Diego, CA, USA.
  - **Lianying Zhao**, Joseph Choi, Didem Demirag, Kevin Butler, Mohammad Mannan, Erman Ayday, Jeremy Clark. One-Time Programs Made Practical. *Financial Cryptography and Data Security 2019 (FC'19)*, Feb. 18-22, 2019, St. Kitts.
  - **Lianying Zhao**, Mohammad Mannan. Hypnoguard: Protecting Secrets across Sleep-wake Cycles. *ACM Conference on Computer and Communications Security (CCS'16)*, Oct. 24-28, 2016, Vienna, Austria.
  - **Lianying Zhao**, Mohammad Mannan. Gracewipe: Secure and Verifiable Deletion under Coercion. *Network and Distributed System Security Symposium (NDSS'15)*, Feb. 8-11, 2015, San Diego, CA, USA.
  - **Lianying Zhao**, Mohammad Mannan. Explicit Authentication Response Considered Harmful. *New Security Paradigms Workshop (NSPW'13)*, Sept. 9-12, 2013, Banff, Canada.
- **Refereed Journal/Magazine Publications**
  - **Lianying Zhao**, David Lie. Is Hardware More Trustworthy than Software? IIEEE Security & Privacy, 18(5): 8–17, Sept.-Oct. 2020.
  - **Lianying Zhao**, Mohammad Mannan. Deceptive Deletion Triggers Under Coercion. *IEEE Transactions on Information Forensics and Security (TIFS)*, 11(12): 2763–2776 (December 2016).
  - Kun Li, Xiuxin Zhu, **Lianying Zhao**. Design of Hardware and Control Software with Wavecom Communication Module Q2406B. *Electronic Measurement Technology*, 4: 95-97, 2006.
- **Patents and Other Refereed Publications**
  - Mohammad Mannan, **Lianying Zhao**. Password triggered trusted encryption key deletion. *U.S. Patent No. 10,516,533*. Dec. 24, 2019.

- Mohammad Mannan, **Lianying Zhao**. Protection System and Method against Unauthorized Data Alteration. *U.S. Patent No. 10,977,381.* Apr. 13, 2021.
- **Lianying Zhao**, Mingqiao Shangguan, Hui Wang, Yonggang Xiao. An Optimized Page Aging Mechanism for Memory Swapping on Android Devices. *IP.COM*, 2013 (IBM).
- **Lianying Zhao**, Mingqiao Shangguan, Hui Wang, Yonggang Xiao. A New Android Low Memory Killer adapted for "User Behavior Analytics" and "Effort to Restart", as well as user customizable. *IP.COM*, 2012 (IBM).

- **Submissions under Review**
  - **Lianying Zhao**, He Shuang, Shengjie Xu, Wei Huang, David Lie. A Survey of Hardware Improvements to Secure Program Execution *ACM Computing Surveys (CSUR).* Submitted in November 2022.
  - Sajjad Pourali, Xiufen Yu, **Lianying Zhao**, Mohammad Mannan, Amr Youssef. A Hijacker's Guide to the Android TLS Galaxy: Attributing Certificate Validation Failures. *Network and Distributed System Security Symposium (NDSS'24).* Submitted in June 2023.
  - Ehsan Khodayarseresht, Sofya Smolyakova, **Lianying Zhao**, Armin Mansouri, Suryadipta Majumdar. ForenThings: An Interactive Framework for Crime Scene Reconstruction in IoT Forensic. *Network and Distributed System Security Symposium (NDSS'24).* Submitted in June 2023.

## Highly Qualified Personnel

- **Ph.D. Student** - Saeid Ghasemshirazi, Starting January 2024
- **Master's Thesis Students** - Yusef Karim, September 2020 – December 2021
  Muhammad Shafayat Oshman, January 2020 – January 2022
  Ming Lei, September 2021 – Present
  Emma Sewell, September 2021 – Present, Co-supervisor: Dr. Anil Somayaji
  Hossein Asghari, Starting September 2023
  Kamran Dar, Starting September 2023
  Parsa Kootzari, Starting September 2023
  Matthew Nitschke, Starting September 2023
  Jiazhang Wang, Starting September 2023
- **I-CUREUS Interns** - Michael Shlega, September 2021 – December 2021
  Adel Agha, May 2021 – August 2021
  Zacchaeus Leung, May 2020 – August 2020
- **Mitacs Accelerate Intern** - Shubham Chander, January 2020 – June 2020
- **DSRI Intern** - Eduard Patlea, May 2023 – Present
- **Co-supervised Master's** - Md. Shahab Uddin, July 2019 – August 2021, Co-supservisor: Dr. Mohammad Mannan, Concordia University
- **Master's Project student** - Segun Odunade, May 2020 – August 2020
- **Undergraduate Research Interns** - Nabil Hossain, May 2022 – August 2022
  Jiazhang Wang, May 2023 – Present
  Matthew Nitschke, May 2023 – Present
- **Bachelor's Honours student** - Soumen Nath, May 2023 – Present
  Braeden Brooking, September 2022 – December 2022
  Sicheng Qiu, May 2022 – August 2022
  Xiaoyu Jia, January 2021 – April 2021
  Zhaohong Wan, May 2020 – August 2020
  Cole Macdonald, September 2019 – December 2019

- **Unofficially Co-supervised** - He Shuang, September 2019 – Present, Ph.D., U of T
  Xiufen Yu, September 2021 – Present, Master's, Concordia
  Supraja Baskaran, January 2022 – Present, Master's, Concordia
  Sajjad Pourali, September 2020 – Present, Ph.D., Concordia

## Teaching and Lecturing

- **Courses taught**
  *Carleton*
  - COMP 3000A/B: Operating Systems (Winter 2023), 348 students
  - COMP 5900H: Trusted Computing and Emerging Attacks (Fall 2022)
  - COMP 3000A/B: Operating Systems (Winter 2022), 332 students
  - COMP 5900H: Trusted Computing and Emerging Attacks (Fall 2021)
  - COMP 5900X: Trusted Computing and Emerging Attacks (Winter 2021)
  - COMP 3000: Operating Systems (Winter 2021), 330 students
  - COMP 5900X: Trusted Computing and Emerging Attacks (Winter 2020)
  - COMP 3000: Operating Systems (Fall 2020), 250 students

- **Teaching assistantship**
  *Concordia*
  - SOEN 321: Information Systems Security (Fall 2015)
  - INSE 6120: Cryptographic Protocols and Network Security (7 terms)

- **Other lecturing**
  *Active IBM university instructor on mainframe technologies*
  - Teaching the students: frequent *Blue Power Station* sessions
    Universities visited: WHU, SEU, YNU, HUST, TONGJI, PKU, SCUT, SZU, DJTU, UESTC, NEU, etc.
  - Teaching the teachers (T3): 5-day faculty training workshop for the Open University of Hong Kong

## Professional Services

**PC Member**: IEEE Symposium on Security and Privacy (S&P 2023)
**PC Member**: IEEE Symposium on Security and Privacy (S&P 2024)
**PC Member**: ACM Conference on Computer and Communications Security (CCS 2023)
**PC Member**: USENIX Workshop on Cybersecurity Experimentation and Test (CSET 2023)
**PC Member**: International Symposium on Foundations  Practice of Security (FPS 2022)
**PC Member**: International Conference on Privacy, Security, and Trust (PST) 2022

**Reviewer for journals:**
Elsevier Computers & Security, 2021
IEEE Security & Privacy, 2020, 2021
IEEE Transactions on Network and Service Management (TNSM), 2022
IEEE Transactions on Information Forensics and Security (TIFS), 2022

**Reviewer for grant proposals:**

Mitacs Elevate, 2020
Mitacs Accelerate, 2021
NSERC — Discovery Grant (DG), 2022
NSERC — Alliance, 2022

## Languages

**Chinese** (Mandarin): Native proficiency – ILR5
**English**: Full professional proficiency – ILR4
**French**: Professional working proficiency – ILR3

## Community and Media Recognition

- Invited Talks
  - 2021/04/16: On the Application of Hardware Security Mechanisms to Counter "Unconventional" Threats, IBM Research Security & Privacy PIC Seminar, IBM T.J. Watson Research Center (Virtual)
  - 2021/02/16: Reflections on the Trustworthiness of Hardware in Computer Security, Joint CRI and IPSI Public Lecture Series, University of Toronto (Virtual)
- Broadcast Interview
  - 2019/07/29: Concordia researchers developing software to fight ransomware, CTV News, CTV Montreal
- Text Interviews
  - 2017/02/06: New Security Advances Bridge the Gap Between Software and Hardware, All About Circuits
  - 2016/11/29: The security software you probably don't need - but Donald Trump does, The Daily Dot
  - 2016/11/28: Now safeguard your laptop's data even when it goes to sleep, PC Magazine
  - 2016/11/23: How to Protect Your Laptop - Even When It's Asleep, ACM Technews