Carleton UNIVERSITY | Department of Systems and Computer Engineering

SYSC 4810
Introduction to Network and Software Security

Calendar description

Fundamental concepts, terminologies, and theories of computer security; principles underlying common security controls; various types of threats and attacks on networks and software systems, how they work, and controls for dealing with them; security risk assessment and management; legal and ethical aspects of computer security.

Includes: Experiential Learning Activity.

Lectures three hours a week, problem analysis one and a half hours a week.

http://calendar.carleton.ca/undergrad/courses/SYSC/

Prerequisites

Fourth-year status in Communications, Computer Systems or Software Engineering.

Precludes additional credit for COMP 4108.

Prior knowledge

Students should have knowledge of:

- Basic number theory (e.g., prime numbers)
- Numeral systems (e.g., binary, decimal, hexadecimal)
- Basic set theory
- Computer organization (e.g., execution stacks)
- TCP/IP networking concepts
- Programming skills (in C)

Course objectives

Concerns related to the security of modern computer systems and networks, and the information that they use, store, and communicate, are becoming more commonplace in our daily lives. Systems today are comprised of broad and heterogeneous communication networks with many interacting software and hardware components that can be spread across a variety of application domains, each with their own security concerns with varying implications and priorities. For example, smartphones, wearable health-monitoring devices, GPS navigation devices, automobiles, energy grid services, and even home appliances like washers and dryers now come with Internet connections by which data from and about the user goes to places where users have little visibility or control. On one hand, users want the convenience and benefits that added connectivity

brings, while on the other hand, they are growing increasingly worried about the threat and impact of suffering massive losses of their personal data and information. Computer security brings these two threads together as technology races forward with \smart" products that all too often omit the basic controls that can prevent or limit security attacks and failures.

This course examines the fundamentals of network and software security, and explores the central problems that confront security designers and administrators including defining the threats to computer and network systems, evaluating the relative risks of these threats, and developing effective countermeasures and controls.

The course is intended to cover a broad spectrum of network and software security fundamentals, while striking a balance between theory and practice. It will provide students with the foundation and skills needed to become security-conscious engineers.

List of topics

- Security Concepts: Confidentiality, Integrity, Availability, Threats, Attacks, Assets.
- Fundamental Security Design Principles.
- Attack Surfaces and Attack Trees.
- Security Strategies, Policies, and Implementations: Prevention, Detection, Recovery.
- Cryptography: Symmetric vs. Asymmetric, Hashing, Digital Signatures, Key Management.
- User Authentication: Passwords, Tokens, Biometrics.
- Access Control Principles: Subjects, Objects, Access Rights, Role-Based vs. Attribute-Based.
- Trusted Computing and Multilevel Security.
- Malicious Software: Viruses, Worms, Trojans, Bots, Spam, Phishing, Backdoors, Rootkits.
- Intrusion Detection, Firewalls, and Intrusion Prevention Systems.
- Internet Security Protocols and Standards: SSL, TLS, HTTPS, IPSec.
- Internet Authentication Applications: Kerberos, Certificates, Public-Key Infrastructure.
- Wireless Network Security and Mobile Device Security.
- Software Security: Buffer Overflows, Handling Inputs/Outputs, Secure Programming.
- System Security: Operating Systems, Cloud, IoT Security.
- Security Management, Risk Assessment, and Threat Modeling.
- Security Controls, Plans, and Procedures.
- Security Evaluation and Assurance.
- Legal and Ethical Aspects.

Learning outcomes

By the end of this course, students should know and understand:

- Fundamental concepts, terminologies, principles, and theories of network and software security.
- Primary aspects of a comprehensive security strategy.
- Basic principles underlying the main cryptographic concepts and technologies available today, including symmetric and asymmetric encryption, hashing, and digital signatures.
- Security policies (such as authentication, integrity, and confidentiality), as well as protocols to implement such policies.
- Various types of security threats and attacks on networks and software systems, how they work, and controls for dealing with them.
- Relevant personnel, legal, and ethical issues related to network and software security.

By the end of this course, students should be able to:

- Identify the types of threats and attacks that apply to different categories of computer and network assets.
- Identify suitable countermeasures and security controls for dealing with specific types of threats and attacks.
- Analyze and specify security properties of simple computing systems.
- Implement and use basic security tools to enhance network and software security.
- Develop basic security enhancements in stand-alone applications.

Graduate Attributes (GAs)

The Canadian Engineering Accreditation Board requires graduates of engineering programs to possess 12 attributes at the time of graduation. Activities related to the learning outcomes listed above are measured throughout the course and are part of the department's continual improvement process. Graduate attribute measurements will not be taken into consideration in determining a student's grade in the course. For more information, please visit: https://engineerscanada.ca/.

Graduate Attribute	Learning outcome(s)
1.8.S Knowledge Base: Developed: Software engineering	1-6
2.1: Problem Analysis: Developed: Problem Definition	7
2.2: Problem Analysis: Developed: Approach to the Problem	8
4.4: Design: Developed: Design solution(s)	9-11
7.1: Communication Skills: Developed: Instructions	

Accreditation Units (AUs)

For more information about Accreditation Units, please visit: https://engineerscanada.ca/.

The course has a total of 46 AUs, divided into:

- Engineering Science: 60%
- Engineering Design: 40%

Instructor and TA contact

Specific to course offering (tbd)

Textbook (or other resources)

Specific to course offering (tbd)

Evaluation and grading scheme

Specific to course offering (tbd)

Breakdown of course requirements

Specific to course offering (tbd)

Tentative week-by-week breakdown

Specific to course offering (tbd)

General regulations

Specific to course offering (tbd)