CyberSEA Research Lab
Carleton University
https://carleton.ca/cybersea/
@CyberSEA_Lab

Systems and Computer Engineering
Carleton University
1125 Colonel By Drive
Ottawa, ON K1S 5B6

December 11, 2021

Position Available: Ph.D. Candidate

Cyber 360: A Cyber Risk Visualization and Action Platform

The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab at Carleton University is actively looking for a graduate student at the Doctoral level to work on a Mitacs-funded research project starting in September 2022 or sooner. This project will be conducted in collaboration with BankingBook Analytics (BBA).

Project Description

As systems and organizations become larger and more complex, decision-makers face many challenges regarding ways to identify, analyze, and prepare for threats and hazards, mitigate vulnerabilities, and minimize impact and consequences. This project aims to develop a cyber risk dashboard that supports asset management, threat source identification, and advanced threat assessment techniques to identify and score security vulnerabilities related to the people, processes, and systems of an organization. The project also aims to map mitigation strategies with identified vulnerabilities, and where such mitigation strategies does not exist, create enterprise-wide projects to develop and requisition internally and externally. The internal rate of return (IRR) or economic value of the outcomes of such mitigation strategies will be monitored to provide additional insights.

In this project, we will focus on developing a software platform to manage and store threat model information and integrate with BBA's machine learning models to provide insights into potential cyber risks. We will use a well-known and established threat modeling methodology such as STRIDE to obtain a set of threats (or classes of threats) that need to be mitigated. We will also use a suitable vulnerability scoring framework such as CVSS (or other econometric scoring models) to score the identified vulnerabilities and obtain data that can be ingested by existing machine learning models to produce projected loss severity outcomes.

Project Keywords:

- cybersecurity
- threat modeling
- security metrics
- risk assessment
- data science
- visualization
- programming

Objective

The general objective of the project is to develop a solution capable of providing more objective, reproducible, consistent, commonly understandable, and actionable information that can integrate with existing machine learning models to assist stakeholders in making decisions on how to improve overall organizational security and resilience. This will involve the following tasks:

(1) Developing an approach to identify/inventory the relevant assets, threat sources, and vulnerabilities for a complex organization;

(2) Establishing a mechanism/approach for scoring the identified vulnerabilities to generate actionable data that can support decision-making and be used as input for more detailed data-analysis methods; and

(3) Implementing a cyber risk dashboard to manage and visualize the data, and provide recommendations and guidance on how to improve the organizational security and resilience.

Related Literature References

[1] L. Tullo, S. Zernov, S. Farooq, and D. Gong. Distribution Analysis for Information Risk (DAIR): A Cyber Quantification Framework. Global Risk Institute White Paper, October 2019.

[2] J. Boehm, N. Curcio, P. Merrath, L. Shenton, and T. Stähle. The Risk-Based Approach to Cybersecurity. McKinsey & Company White Paper. October 2019.

[3] L. Matta and M. Husák. A Dashboard for Cyber Situational Awareness and Decision Support in Network Security Management. 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), pages. 716-717, 2021.

[4] N. Jones and B. Tivnan. Cyber Risk Metrics Survey, Assessment and Implementation Plan. The Homeland Security Systems Engineering and Development Institute (HSSEDI) Technical Report AD1108439. May 2018.

[5] A. Shostack. Threat Modeling: Designing for Security. John Wiley & Sons, 2014.

[6] P. Mell, K. Scarfone, and S. Romanosky. The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems. NIST Interagency Report 7435, National Institute of Standards and Technology, August 2007.

Desired Skills/Qualifications

Suitable candidates will have a Master's degree in Software Engineering, Computer Science, or a related field. Ideal candidates will be self-motivated with an ability to work independently and to communicate effectively in a team environment. Applicants must possess strong programming skills. A background in cybersecurity is highly desirable. Experience with threat modeling, threat and risk assessment, and/or knowledge of security metrics and measures is considered an asset. Applicants should also have very strong written and verbal communication skills.

All candidates must satisfy the Minimum Admission Requirements for Doctoral Programs at Carleton University. International candidates must also ensure that they satisfy the English as a Second Language Requirements. In all cases, these requirements will be strictly enforced when evaluating an application for admission.

Funding

Successful candidates for this position will be *eligible for funding* in the form of a research assistantship. Specific funding details are determined at the time of offer and consider numerous factors such as academic standing, research potential, availability of funds, eligibility for teaching assistantship and/or scholarships, etc.

Host Research Institute Information

Carleton University is a public comprehensive university, founded in 1942, in Ottawa, Ontario, Canada. The research-intensive Faculty of Engineering and Design at Carleton University is recognized as one of Canada's leading institutions in the study and research of engineering, architecture, industrial design and information technology. Since the inception of engineering at Carleton in 1945, our experts have pushed the bounds of innovation and discovery. Carleton focuses on anticipating the needs of industry and society, and offers forward-thinking programs with real world application and produces research that is helping to shape our present and future. The Department of Systems and Computer Engineering is a recognized world-class institution in software engineering, computer systems engineering, communications engineering, and biomedical engineering. Together with the Department of Electronics, the Department of Systems and Computer Engineering constitutes one of the largest and most research-intensive centres for Electrical and Computer Engineering and Software Engineering education and research in Canada. The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab conducts advanced academic research to develop systematic and rigorous approaches for evaluating and assuring the cyber security of software-dependent systems.

Further Information

For more information about Graduate Studies at Carleton University and the Department of Systems and Computer Engineering, please visit: https://carleton.ca/sce/graduate-studies/. For more information about applying for Graduate Studies at Carleton University, please visit: https://graduate.carleton.ca/apply-online/. For more information about funding for Graduate Studies, please visit: https://graduate.carleton.ca/financial-assistance/admissions-funding/.

How to Apply

Interested applicants are to send a **CV** and **Statement of Interest** detailing your research interests, background, and experience by email to the CyberSEA Lab Director:

Jason Jaskolka, Ph.D., P.Eng.

Systems and Computer Engineering | Carleton University
Canal Building 6206 | 1125 Colonel By Drive | Ottawa, ON K1S 5B6
☎ +1 (613) 520-2600 Ext. 1873
✉ jason.jaskolka@carleton.ca
https://carleton.ca/jaskolka/
https://www.linkedin.com/in/jason-jaskolka-160ab434/
@JasonJaskolka

For more information about how to apply, please visit: https://carleton.ca/cybersea/positions-available/

Application Deadline

Applications will be reviewed as they arrive until a suitable candidate is found.