CyberSEA
Research Lab
Carleton University

Carleton
University

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: M.A.Sc./Ph.D. Candidate

Human-Centric Cyber Security Standardization

The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab at Carleton University is actively looking for a graduate student at the Doctoral or Master's level to contribute to a funded research project starting in September 2022.

Project Description

Cyber security standards and guidelines related to secure system development and management play a critical role in security assurance, certification, and evaluation. Effective security assurance often demands compliance with domain-relevant cyber security standards. As a result, standards are seen to be important in the ensuring minimum levels of safety in many arenas, but how much do we know about the role technical and regulatory standards play in promoting cyber security practices and fostering cyber-resilience?

There is reason to believe that standardization is perceived differently by different human actors involved in secure system development. Some may find cyber security standardization useful, while others find it a waste of time. Maybe it is not well understood why something is standardized the way it is? Maybe it seems completely arbitrary? Sometimes too, it is a question of *incentives*. It may be unclear whether anyone checks or cares and this may depend on the criticality of the kinds of systems being built. Are there any tangible benefits to comply with the standards? How can we get everybody working together to provide a sort of compliance work flow with standards that makes sense for the parties involved and that are understandable by the parties involved? Engineers think very differently about these problems than policymakers and legislators do. Often, these groups have similar goals and objectives, but they do not "speak the same language." This prevents the realization of the mutual benefits of their individual contributions. It is important to have people from different backgrounds to work together to operationalize cyber security principles and practices.

This project will investigate how cyber security standards differ between sectors, how interpretable those standards are, and how to those standards and related regulations interact to create a level of cyber resilience.

Project Keywords:

- cyber security
- cyber resilience
- standards
- guidelines
- best practices
- security policy
- security assurance

Objectives

This project seeks to investigate how to standardize cyber security in a SMART (specific, measurable, attainable, repeatable, and time-dependent) way. This will involve the following activities and tasks:

(1) Performing a literature survey of existing standards, guidelines, regulations to try to identify the cross-sections on which to focus;

(2) Conducting surveys, questionnaires, and/or interviews to better understand perceptions of standards in regulation and to collect the information needed to understand the ways in which the standards can be improved;

(3) Developing a measurement framework by which empirical evidence can be generated to support compliance with standards; and

(4) Providing actionable recommendations based on the data collected to suggest how to improve cyber security standardization.

Related Literature References

[1] J. Jaskolka. Recommendations for effective security assurance of software-dependent systems. In K. Arai, S. Kapoor, and R. Bhatia, editors, *Intelligent Computing, SAI 2020*, volume 1230 of Advances in Intelligent Systems and Computing, pages 511–531. Springer, Cham, July 2020.

[2] L. Shan, B. Sangchoolie, P. Folkesson, J. Vinter, E. Schoitsch, and C. Loiseaux. A survey on the applicability of safety, security and privacy standards in developing dependable systems. In A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, and F. Bitsch, editors, *Computer Safety, Reliability, and Security*, pages 74–86, Springer, Cham, 2019.

[3] C.W. Axelrod. The creation and certification of software cybersecurity standards. In *Proceedings of the 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY, pages 1-6.

[4] J. Weidman, I. Bilogrevic, and J. Grossklags. Nothing standard about it: An analysis of minimum security standards in organizations. In I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, and A. Sasse, editors, *Computer Security*, pages 263–282, Spinger, Cham, 2020.

[5] P. Wagner, G. Hansch, C. Konrad, K.-H. John, J. Bauer, and J. Franke. Applicability of security standards for operational technology by SMEs and large enterprises. In *25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, pages 1544–1551, September 2020.

[6] A. Colombo and B. Karney. Why engineers need public policy training and practice. *The Journal of Policy Engagement*, 1(1):9-12, 2009.

Desired Skills/Qualifications

Suitable candidates will have a Bachelor'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. background in computer security is highly desirable. Experience with standards, as well as skills in data collection, conducting surveys, and data analysis is considered an asset.

All candidates must satisfy the Minimum Admission Requirements 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/
in 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.