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

August 19, 2021

Position Available: Ph.D. Candidate

Formal Architecture Models Supporting Security Requirements Traceability and Compliance-By-Design for Low-Earth Orbit Satellite Operations

The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab at Carleton University is actively looking for a graduate student at the Doctoral level to join a Mitacs-funded research project in January 2022. The project will be conducted in collaboration with Telesat.

Project Description

Low-earth orbit (LEO) satellite constellations and their associated segment systems and networks promise global connectivity with high throughput, low latency, and improved economics. Such systems demand increased levels of security and resilience to provide assured services to customers. As a result, compliance with a variety of security standards, policies, and regulations is required and must be demonstrable throughout the system development lifecycle (SDLC) for these systems to develop customer trust and find widespread use. However, there are numerous challenges associated with effectively maintaining the traceability of specifications and security controls during system design and beyond to support security assurance and audit activities. The traceability of this compliance is a common problem in the industry and is expected to become increasingly challenging as these systems evolve. Thus, there is a need for a systematic way to validate and trace the application and compliance of cybersecurity controls mandated by such standards and regulations throughout the lifecycle of large and complex systems.

This project seeks to use model-based systems engineering (MBSE) approaches to develop an architecture and design framework to support the traceability of compliance requirements to the architecture design of the operations segment of Telesat's LEO system. The operations segment connects the overall LEO system by orchestrating the space and ground segments to deliver the service. It combines central control and local intelligence to optimize performance. The expected outcome is an architecture metamodel with standardized interfaces supporting traceability and compliance-by-design for cybersecurity standards, similar to what AUTOSAR has become in the automotive domain.

Project Keywords:

- security
- model-based systems engineering
- formal methods
- architecture design
- metamodel
- compliance
- standards
- requirements traceability
- satellite constellation
- operations segment

Objective

This PhD thesis contributes to development of a standardized architecture design framework for the operations segment of low-earth orbit satellite constellations supporting compliance-by-design for cybersecurity standards. This will involve identifying the set of security requirements from relevant standards, designing and specifying a security compliance-by-design architecture framework and design methodology for a LEO satellite operations segment. It will also involve performing security analyses of the developed architecture framework and developing traceability support for demonstrating security compliance among LEO operations segment architecture components.

Related Literature References

[1] J. M. Willis, R. F. Mills, L. O. Mailloux, and S. R. Graham. Considerations for secure and resilient satellite architectures. In *2017 International Conference on Cyber Conflict (CyCon U.S.)*, pages 16–22, November 2017.

[2] Committee on National Security Systems. National information assurance policy for space systems used to support national security missions. CNSS Policy 12, Committee on National Security Systems, November 2012.

[3] Q. Rouland, B. Hamid, and J. Jaskolka. Formal specification and verification of reusable communication models for distributed systems architecture. *Future Generation Computer Systems*, 108:178–197, July 2020.

[4] J. L. de la Vara, A. Ruiz, K. Attwood, H. Espinoza, R. K. Panesar-Walawege, A. L'opez, I. del Río, and T. Kelly. Model-based specification of safety compliance needs for critical systems: A holistic generic metamodel. *Information and Software Technology*, 72:16–30, 2016.

[5] 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, 2020.

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. A background in computer security and model-based systems engineering (MBSE) is highly desirable. Experience with formal specification and verification, requirements engineering, software architecture and design, and/or knowledge of cybersecurity stadards, guidlines, and regulations 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.