Institut de Recherche
en Informatique de Toulouse
CNRS - INP - UT3 - UT1 - UT2J

Centre National de la Recherche Scientifique
Institut de Recherche en Informatique de Toulouse
118 Route de Narbonne
31062 Toulouse CEDEX 9

Carleton UNIVERSITY
Canada's Capital University
Systems and Computer Engineering
Carleton University
1125 Colonel By Drive
Ottawa, ON K1S 5B6

June 17, 2020

Position Available: Ph.D. Candidate (Cotutelle)

Security Assurance Cases within System and Security Co-evolution in Cyber-Physical Systems

A cotutelle PhD position is available jointly between the Institut de Recherche en Informatique de Toulouse (IRIT) in Toulouse, France and Carleton University in Ottawa, ON, Canada starting in September 2020.

Project Description

A Cyber-Physical System (CPS) integrates computing and communication capabilities with the monitoring and control of entities in the physical world. Components of CPSs are remotely deployed, have many constraints, e.g., Small Weight and Power (SWaP), may be physically inaccessible for maintenance, and/or physically accessible for attack. Examples can be found in transportation systems, smart power grids, health monitoring, and many other critical infrastructures. Often, CPSs are critical systems from both safety and security aspects: their failure can endanger lives or cause large economic losses. In a context of fast changing cybersecurity threats, and ever-emerging vulnerabilities, long-lived CPSs require a high level of maintainability, to ensure continuous (safe) service, and minimal maintenance costs. Safety-critical systems are usually accredited or certified. Maintenance in secure conditions (e.g., security patch installation) should be possible without having to re-accredit or re-certify the CPSs. Currently some security patches on CPSs are simply skipped because modifying the code, or updating an anti-virus database, would require running the accreditation or certification process anew. This situation is not sustainable.

Objective

This PhD thesis contributes to this matter by describing a methodological tool support to build and reuse security assurance cases in the form of reusable models in the context of system architecture and security co-evolution. This will involve developing an argumentation structure for reasoning about the security of these systems and developing approaches to generate sufficient evidence to support the claims in the argument. Subsequently, this thesis offers guidelines for generating explanations and evidence to be communicated to, understood by, and acceptable to regulatory authorities, certification bodies, and the eventual users of the systems.

Related Literature References

[1] B. Hamid and D. Weber. Engineering secure systems: Models, patterns and empirical validation. *Computers & Security*, 77:315–348, 2018.

[2] J. Jaskolka. Challenges in assuring security and resilience of advanced metering infrastructure. In *18th Annual IEEE Canada Electrical Power and Energy Conference*, EPEC 2018, pages 1–6, 2018.

[3] L. Amgoud. Postulates for logic-based argumentation systems. *International Journal of Approximate Reasoning*, 55(9):2028–2048, 2014.

[4] E. Denney and G. Pai. Tool support for assurance case development. *Automated Software Engineering*, 25(3):435–499, 2018.

[5] E.K.H. Fong and D.A. Wheeler. A sample security assurance case pattern. IDA Paper P-9278, Institute for Defense Analyses, Alexandria, VA, U.S.A., December 2018.

[6] S. Yamamoto and Y. Matsuno. An evaluation of argument patterns to reduce pitfalls of applying assurance case. In *1st International Workshop on Assurance Cases for Software-Intensive Systems (ASSURE)*, pages 12–17, 2013.

Desired Candidate 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 logic and discrete mathematics, computer security, software/system modelling and software engineering processes and concepts is highly desirable. Experience with assurance/certification approaches and techniques, software maintenance and evolution, and reasoning is considered an asset.

All candidates must satisfy the Minimum Admission Requirements for Doctoral Programs at IRIT and the Minimum Admission Requirements for Doctoral Programs at Carleton University.

What is a Cotutelle?

A cotutelle is the French term for "Joint Enrolment". This refers to a bilateral doctoral enrolment/co-enrolment and exchange agreement between two universities (the home university and the partner university) in different countries. Under such an arrangement, a doctoral student completes all of the requirements of the PhD program in both the home and partner university, and conducts his/her dissertation research collaboratively, sequentially, and for roughly equal amounts of time in both universities and is supervised by a faculty member from each of the universities. The dissertation will be examined by a committee whose members are drawn from both institutions.

Students completing a cotutelle will graduate with a single PhD degree from both the home and partner institution. This typically occurs with the student receiving a diploma from each university, each carrying a notation that the degree was obtained through a cotutelle agreement. A cotutelle offers you a unique international experience adding significant value to your PhD degree.

Host Research Institute Information

The Institut de Recherche en Informatique de Toulouse (IRIT), created in 1990, is a Joint Research Unit (UMR) of the Centre National de la Recherche Scientifique (CNRS), the Institut National Polytechnique de Toulouse, the Université Paul Sabatier, the Université Toulouse 1 Capitole and the Université de Toulouse Jean Jaurès. IRIT is one of the largest UMR at the national level, is one of the pillars of research in Occitanie with its 700 members, permanent and non-permanent. The Advancing Rigorous Software and System Engineering (ARGOS) team's main research topics are rigorous system and software engineering processes, security and resilience at both the foundations and application level, particularly for cyber-physical systems. The Argumentation, Décision, Raisonnement, Incertitude et Apprentissage (ADRIA) team contributes to the development of new approaches to knowledge representation, reasoning and decision in Artificial Intelligence.

Carleton University is a public comprehensive university, founded in 1942, in Ottawa, Ontario, Canada. The research-intensive Faculty of Engineering and Design is recognized as one of Canada's leading institutions in the study and research of engineering, architecture, industrial design and information technology. 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. The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab conducts research to develop systematic and rigorous approaches for evaluating and assuring the security of software-dependent systems.

Supervision

Brahim Hamid (IRIT); Leila Amgoud (IRIT); Jason Jaskolka (Carleton)
(brahim.hamid@irit.fr; leila.amgoud@irit.fr; jason.jaskolka@carleton.ca)

Application Instructions and Further Information

To apply, please send your CV to: brahim.hamid@irit.fr and jason.jaskolka@carleton.ca

Administrative Process

2 to 3 months after the acceptance.