Introduction: Cybersecurity and Software Assurance Minitrack

Luanne Chamberlain, Richard George,
Thomas Llansó
Johns Hopkins Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
Luanne.Chamberlain, Richard.George,
Thomas.llanso@jhuapl.edu

Tyson Brooks
School of Information Studies
Syracuse University
343 Hinds Hall
Syracuse, NY13244
ttbrooks@syr.edu

Despite increased awareness of the cyber threat and growing investments in improved defenses, cyber attackers continue to widen their asymmetric lead over defenders. As an unending stream of media reports demonstrate, cyber-intensive systems of all varieties are targets, including not just traditional enterprise IT, but internet-of-things devices and critical infrastructure systems as well.

Given this situation, the goal of this minitrack is to develop science foundations, technologies, and practices that can improve the security and dependability of complex systems. The papers for the mini-track come at this goal from a variety of perspectives, including the behavior of red team members on systems that use deception techniques, extending authentication via measurement of user behaviors, observing intruders by transferring their activity to a benign environment, evaluting the usability of an API designed to counter cross-site scripting attacks, assessing whether security properties are maintained in self-adaptive security systems, and conducting multi-objective selection of security defenses using weighted factors.

In the first paper, *Protecting Temporal Fingerprints with Synchronized Chaotic Circuits,* Fengyi Tang and Betty H.C. Cheng, both from the Department of Computer Science and Engineering at Michigan State University, propose a novel cryptographic framework that protects information embedded in ECU network communications by delivering an encryption system that periodically "salts" the temporal dynamics of individual ECU units with chaotic signals that are difficult to learn. Their framework aims to protect ECU networks from an especially insidious class of attacks called 'nudging attackers.'

In the second paper, *Measuring Confidence of Assurance Cases in Safety-Critical Domains*, authors Chung-Ling Lin and Wuwei Shen, both of Western Michigan University, and Betty H.C. Cheng from Michigan State University, discuss how advances in uncertainty theories and software traceability can be synergistically combined and leveraged to help automate software certification. The paper concerns the area of assurance cases (ACs) and the need to help automate the evaluation of ACs based on prior evaluations of similar ACs done by human certifiers. The authors introduce a framework called DS4AC that employs Dempster-Shafter theory in the AC context. The paper then illustrates DS4AC using examples, including one called "Coupled Tanks".

In the third paper, *Synthesis of Verified Architectural Components for Critical Systems Hosted on a Verified Microkernel*, authors David Hardin and Konrad Slind from Collins Aerospace and Johannes Aman Pohjola and Michael Sproul from Data61/CSIRO, Australia examine highly automated synthesis techniques for high-assurance components implementing formally verified security-enhancing architectural transformations for critical systems. They provide evidence, in the form of formal proofs, that these transformations actually do improve key security, as well as safety, properties.

In the fourth and final paper*, Matching Possible Mitigations to Cyber Threats: A Document-Driven Decision Support Systems Approach,* authors Martha Wagner McNeil, Cherie Bakker Noteboom, Jun Liu and Omar El-Gayar, all from Dakota State University and Thomas Llansó of the Johns Hopkins University Applied Physics Lab, present a novel machine learning method for automatically mapping mitigations to cyber threats. They discuss a semi-automated method to produce a starting list of possible mitigations to cyber threats which can flow into mitigation optimization techniques.

URI: https://hdl.handle.net/10125/64518
978-0-9981331-3-3