Introduction: Cybersecurity and Software Assurance Minitrack

Luanne Chamberlain
Johns Hopkins University
Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
luanne.burns@jhuapl.edu

Richard George
Johns Hopkins University
Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
richard.george@jhuapl.edu

Thomas Llansó
Johns Hopkins University
Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
thomas.llanso@jhuapl.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, *The Tularosa Study: An Experimental Design and Implementation to Quantify the Effectiveness of Cyber Deception*, Kimberly J. Ferguson-Walter (U.S. Department of Defense) and nine other co-authors from the U.S. Department of Defense, Texas Tech University and Sandia National Laboratories take up the issue of red team member behavior in a network where deception-based defensive techniques are present. They observed 130 red teamers, employed a survey instrument, and made physiological measurements. The paper offers preliminary results based on a cognitive battery/personality assessment.

In the second paper, *Augmenting Authentication with Context-Specific Behavioral Biometrics*, authors Haoruo Zhang, Digvijay Singh, and Xiangyang Li, all from the Information Security Institute at Johns Hopkins University, were interested in whether behavioral biometric authentication in the context of a specific application/system is feasible in helping to identify fraudulent users. The authors conducted a case study in which they collected and analyzed user biometric behavioral data while users operated a webmail program. The results showed that user behavioral biometrics can, with certain caveats, augment authentication in an application context.

In the third paper, *Cyber Deception Architecture: Covert Attack Reconnaissance Using a Safe SDN Approach*, authors Toru Shimanaka and Ryusuke Masuoka from Fujitsu System Integration Laboratories and Brian Hay from Virginia Tech, explored an approach for observing threat actor behavior by transferring attacker activity to a deception network in a manner undetectable by the actor. The approach involves a packet rewriting technique that uses Software Defined Networking (SDN). The researchers then successfully tested the approach in a war gaming environment.

In the fourth paper, *Fighting Against XSS Attacks. A Usability Evaluation of OWASP ESAPI Output Encoding*, authors Chamila Dilshan Wijayarathna and Nalin A. G. Arachchilage from of the University of New South Wales, examine the usability of an API that helps defend against XSS attacks. The approach involved studying programs written by ten software developers using the API and assessing the programs they wrote. The study revealed three common programmer mistakes and API sixteen usability issues.

In the fifth paper, *Evaluating Security Assurance Case Adaptation*, University of Tulsa authors Sharmin Jahan, Allen Marshall, and Rose Gamble propose a method for assessing the degree of assurance that a security control remains compliant in a system that self-adapts during run-time. The approach involves representing security controls as assurance cases. The results show that it is feasible to map security controls to softgoals and vary satisficing levels during control adaptation.

In the sixth paper,, *Multi-Criteria Selection of Capability-Based Cybersecurity Solutions*, authors

Thomas Llansó and Martha McNeil from the Johns Hopkins University Applied Physics Laboratory and Cherie Noteboom from Dakota State University discuss the challenge of assisting security engineers in selecting defensive solutions in a complex tradespace of potentially competing priorities. The approach involves selecting the best security solutions based on a set of weighted selection factors that have both local and system-wide scope. Preliminary results show that the approach scales well to systems of large size.

In the seventh and final paper, *Data-driven Selection of Security Application Frameworks During Architectural Design*, authors Humberto Cervantes of Universidad Autónoma Metropolitana - Iztapalapa, Junsung Cho, Geumhwan Cho, Hyoungshick Kim of Sungkyunkwan University, Rick Kazman of University of Hawaii at Manoa, Jina Kang of National Security Research Institute, and Jungwoo Ryoo of Pennsylvania State University at Altoona, investigate the criteria used by practicing software architects in selecting security frameworks. They propose how information associated with some of the criteria that are important to architects can be obtained manually or in an automated way from online sources such as GitHub. They identify measures associated with these criteria that can be helpful in providing support for architects to select software frameworks.