Introduction: Cybersecurity and Software Assurance Minitrack

Luanne Burns Goldrich
JHU Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
luanne.burns@jhuapl.edu

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

Thomas Llansó
JHU Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
thomas.llanso@jhuapl.edu

Determined adversaries continue to have the upper hand in their ability to attack cyber-intensive systems, often at will. Even the most causal perusal of industry reports reveals increasing attack frequency and business/mission consequences for affected organizations and individuals. Whether the focus is traditional enterprise IT environments or cyber-physical systems, the asymmetry between attackers and defenders remains a serious problem.

Against this backdrop, the goal of this minitrack is to advance science foundations, technologies, and practices that can improve the security and dependability of complex systems. The papers for the minitrack come at this goal from a diverse set of perspectives, from protecting memory within machines, reducing vulnerabilities in distributed system interactions, deploying more powerful anomaly detection, and assisting cybersecurity engineers in addressing cyber risk and related mitigations.

In the first paper, *Present but unreachable: reducing persistent latent secrets in HotSpot JVM*, authors Adam Pridgen, Simson Garfinkel, and Dan Wallach take up the issue of potential confidentiality breaches for data held in Java virtual machine memory. They illustrate the problem through experiments they ran on existing JVMs, propose stop-gap fixes to existing virtual machines, and advance a new approach for efficient heap sanitization for future JVM designs

In the second paper, *Identifying Implicit Component Interactions in Distributed Cyber-Physical Systems*, authors Jason Jaskolka and John Villasenor discuss the problem of how to detect implicit interactions among components of complex cyber-physical systems. They do so via novel application of an algebraic modeling framework that identifies such interactions as a step towards recognizing and addressing related vulnerabilities.

In the third paper, *A Parallel Outlier Detection Algorithm for Anomaly Detection*, authors Shin-Ying Huang, Ya-Yun Peng, and Fang Yu investigate a similarly challenging problem, that of detecting anomalous behaviors in distributed systems. They propose an anomaly detection algorithm that employs a back propagation neural network. While performance of such approaches is often a concern, the authors propose conducting detection using a parallel processing technique.

In the fourth paper, *BluGen: An Analytic Framework for Mission-Cyber Risk Assessment and Mitigation Recommendation*, authors Thomas Llansó, Martha McNeil, Dallas Pearson, and George Moore focus on cyber risk assessment and mitigations. The authors propose a new approach to analyzing threats and mitigations in terms of base capabilities from which attacks are composed. They develop a set of analytics that are amendable to automation. The analytics assess risk and recommend mitigations based on sensitivity to that risk.

URI: http://hdl.handle.net/10125/41882
ISBN: 978-0-9981331-0-2