Introduction: Cybersecurity and Software Assurance Minitrack

Luanne Burns Chamberlain
JHU Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
luanne.chamberlain@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, *An Empirical Study of Security Issues Posted in Open Source Projects*, authors Mansooreh Zahedi (IT University of Copenhagen), Muhammad Ali Babar (University of Adelaide) and Christoph Treude (University of Adelaide), aim to empirically identify and understand the security issues posted on a random sample of GitHub repositories. They use a mixed-methods approach, combining topic modeling techniques and qualitative analysis. Their findings reveal that the rate of security-related issues is rather small (approx. 3% of all issues), and that the majority of the security issues are related to identity management and cryptography topics. The authors present seven high-level themes of problems that developers face in implementing security features.

In the second paper, *Secure Data Communication via Lingual Transformation*, authors Jeffrey Johnson (Utah State University), Robert Houghton (Idaho State University), Thomas Hilton (University of Wisconsin - Eau Clare) and Kwok Fai Cheah (Utah State University) propose a new form of data communication that is similar to slang in human language. Using the context of the conversation instead of an encryption key, nodes in a network develop a unique alternative language to disguise the real meaning of the communication between them. The authors discuss the potential benefits and challenges in implementing such a system.

In the final paper, *Estimating Software Vulnerability Counts in the Context of Cyber Risk Assessments*, authors Thomas Llansó (Johns Hopkins University Applied Physics Laboratory and Dakota State University) and Martha McNeil (Johns Hopkins University Applied Physics Laboratory) develop and apply a metric to estimate the proportion of latent vulnerabilities to total vulnerabilities in a software system. They then apply the metric to five scenarios involving software on the scale of operating systems. The findings suggest caution in interpreting the results of cyber risk methodologies that depend on enumerating known software vulnerabilities because the number of unknown vulnerabilities in large-scale software tends to exceed known vulnerabilities.

URI: http://hdl.handle.net/10125/50573
ISBN: 978-0-9981331-1-9