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
thomas.llanso@jhuapl.edu

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

The presence of cyber in our daily lives continues its relentless growth with cyber components deeply embedded across an astonishing range of applications, including medicine, finance, transportation, education, agriculture, communications, home automation, social media, voting, the power grid, and many more.

Meanwhile, cyber attackers continue to hold a persistent asymmetric advantage over defenders, a situation that is ever more troubling given cyber's ubiquity. The community increasingly recognizes that the defense of cyber systems is a multi-dimensional challenge that requires new approaches.

The papers in this minitrack provide outstanding examples of the kind of diverse thinking required to strengthen the foundations of cyber defense. The papers cover a range of topics including data sovereignty, moving target defense, vulnerability prediction, malware detection, and attack pattern analysis.

In the first paper, *Utilizing Remote Evaluation for Providing Data Sovereignty in Data-sharing Ecosystems*, authors Favian Bruckner and Falk Howar describe a remote processing approach that arranges for client/customer applications to "travel" to data rather than the other way around. The data processed by the applications remains safeguarded in a controlled environment, with only summary results transmitted back to consuming organizations.

In the second paper, *The use of partially observable Markov decision processes to optimally implement moving target defense*, authors Ashley McAbee, Murali Tummala, and John McEachen discuss an implementation of a partially observable Markov decision process to select among moving target defense options during live attacks. The paper illustrates the approach with a five-state attack sequence.

The third paper, *VULNERLIZER: Cross-analysis Between Vulnerabilities and Software Libraries* authors Irdin Pekaric, Michael Felderer, and Philipp Steinmüller describe a framework for predicting vulnerabilities in software libraries. The approach obtains vulnerability data from the National Vulnerability Database and Vulners and uses software libraries from Docker Debian images maintained in DockerHub for the purpose of training and analysis.

In the fourth paper, *Machine Learning-Based Android Malware Detection Using Manifest Permissions*, authors Jeffrey McDonald, Nathan Herron, William Glisson, Ryan Benton describe an approach that uses machine learning techniques as the basis for identifying Android applications that are, in reality, malware. The target of the machine learning is the manifest file found in an Android application's APK archive.

In the final paper, *Tracing CAPEC Attack Patterns from CVE Vulnerability Information using Natural Language Processing Technique*, authors Kenta Kanakogi, Hironori Washizaki, Yoshiaki Fukazawa, Shinpei Ogata, Takao Okubo, Takehisa Kato, Hideyuki Kanuka, Atsuo Hazeyama, Nobukazu Yoshioka discuss two alternative approaches to finding CAPEC attack patterns related to a vulnerabilities that are logged with a CVE identifier. Such associations can help defenders to understand the implications of new vulnerabilities in terms of how they might manifest during cyber attacks.

URI: https://hdl.handle.net/10125/71459
978-0-9981331-4-0