Cyber Operations, Defence and Forensics

William Bradley Glisson
Sam Houston State University
glisson@shsu.edu

George Grispos
University of Nebraska at Omaha
ggrispos@unomaha.edu

Kim-Kwang Raymond Choo
University of Texas at San Antonio,
raymond.choo@utsa.edu

Abstract

As technology is merged into all aspects of daily life, cyber operations, defences, and digital forensics solutions continue to escalate in importance. This continued escalation necessitates the development of innovative managerial, technological, and strategic analysis solutions. Hence, this mini-track presents research that addresses these needs. The papers in the mini-track investigate the 'Tuning Hyperparameters for DNA-based Discrimination of Wireless Devices', 'HoneyCode: Automating Deceptive Software Repositories with Deep Generative Models', 'Cybersecurity Risk Assessment Framework for Externally Exposed Energy Delivery Systems', and 'Insight from a Containerized Kubernetes Workload Introspection'. The contributions presented in these papers highlight the escalating need for cyber operations, defence, and forensics research.

1. Introduction

The constantly evolving technology landscape demands innovative managerial, technological, and strategic solutions to secure and investigate digitalized civilizations. This mini-track is dedicated to reporting advancements that focus on these emerging and critically important topics. Each paper submission went through a rigorous peer-review process. A summary of each paper is provided below.

2. Wireless Devices Discrimination

In the paper 'Tuning Hyperparameters for DNA-based Discrimination of Wireless Devices' by Bihl et al. [1], the authors investigate hyperparameter optimization for WPAN device identification. More specifically, the paper proposes a method for improving the fingerprinting accuracy of wireless personal area network devices. It presents the results of a comparative study for tuning hyperparameter optimization when using the GRLVQI algorithm as the representative classifier.

3. Automating Deceptive Software

As cyber-attacks continue to cost organizations money, deception becomes an attractive defense strategy. Nguyen et al. [2] investigate the generation of honey code for cyber deception. The authors developed a language-agnostic approach that generates repository structures, human-readable names, and file content. Their solution introduces a tree recurrent network for the overall structure representation as well as generators for names and file content. An automated and scalable synthetic software repository can be used to provide insights into attack tactics and techniques.

4. Externally Exposed Energy

As systems become increasingly integrated with devices like programable logic controllers and supervisory control and data acquisition systems, there is an increasing need to protect critical infrastructure systems. Gouresetti et al. [3] present a relative-risk assessment framework and a software application called MEEDS that can detect exposed operational technology systems. The framework uses data from multiple sources to calculate and present a relative risk score. The proposed solutions can assist organizations with their mitigation plans.

5. Containerized Introspection

The use of containers in cloud environments raises security concerns. In this min-track, Watts et al. [4] present an exploratory case study conducted on a bare-metal cloud that utilizes Kubernetes, the Prometheus, and Apache Spark. Their solution provides empirical data that supports the use of introspection tools as a vehicle to potentially acquiring forensically viable data from different levels of a technology stack.

More specifically, this research investigates the use of an introspection tool across a multi-server stack that utilizes a container. The authors extract the data away

URI: https://hdl.handle.net/10125/71454
978-0-9981331-4-0

from the containerized platform. The results indicate that introspection tools can handle a large, diverse technology stack to gather relevant event reconstruction data.

6. Research roadmap

The papers presented in this mini-track contribute to addressing challenges in Cyber Operations, Defence, and Forensics. However, numerous research challenges remain in these evolving areas.

Future research in these areas includes technology investigations, technical integration, solution impact, and the abuse of technology through attacks, along with the practical analysis and evaluation of proposed solutions. Hence, identifying and validating technical solutions to secure data from new and emerging technologies, investigating the impact that these solutions have on the industry, and understanding how technologies can be abused is crucial to the viability of commercial, government, and legal communities.

7. References

[1] Bihl, T., J. Schoenbeck, C. Rondeau, A. Jones, and Y. Adams, *Tuning Hyperparameters for DNA-based Discrimination of Wireless Devices*, in *Proceedings of the 54th Hawaii International Conference on System Sciences*. 2021, Hawaii International Conference on System Sciences.

[2] Nguyen, D., D. Liebowitz, S. Nepal, and S. Kanhere, *HoneyCode: Automating Deceptive Software Repositories with Deep Generative Models*, in *Proceedings of the 54th Hawaii International Conference on System Sciences*. 2021, Hawaii International Conference on System Sciences.

[3] Gourisetti, S.N.G., M. Touhiduzzaman, T. Ashley, S. Pal, and P. McKenzie, *Cybersecurity Risk Assessment Framework for Externally Exposed Energy Delivery Systems*, in *Proceedings of the 54th Hawaii International Conference on System Sciences*. 2021, Hawaii International Conference on System Sciences.

[4] Watts, T., R. Benton, J. Shropshire, and D. Bourrie, *Insight from a Containerized Kubernetes Workload Introspection*, in *Proceedings of the 54th Hawaii International Conference on System Sciences*. 2021, Hawaii International Conference on System Sciences.