Introduction to the Minitrack on Cyber-of-Things: Cyber Crimes, Cyber Security and Cyber Forensics

William Bradley Glisson
University of South Alabama, USA
bglisson@southalabama.edu

Kim-Kwang Raymond Choo
University of Texas at San Antonio, USA
raymond.choo@fulbrightmail.org

Abstract

The continuous amalgamation of technology into the increasing facets of everyday life are conducive to encouraging cyber-crimes, cyber-security solutions and cyber forensics investigations. Hence, responses that address resulting concerns presented in this mini-track include 'On the Effectiveness of Hardware Enforced Control Flow Integrity', a novel method to enhance ISSP compliant: An approach drawing upon the concept of empowerment in ERM system workflow', and an analysis of 'Short-Term and Long-Term Solutions for Secure Verification of Aircraft Reported ADS-B Location in Air Traffic Networks'. These contributions highlight the growing need to investigate and address cyber security vulnerabilities along with investigating novel solutions to support cyber forensic investigations in the broad context of cyber-of-things.

1. Introduction

The evolving landscape of technology, society and threat landscape demands the development of innovative managerial, technological and strategic solutions to secure our increasingly digitalized society. This mini-track is dedicated to reporting the state-of-the-art and recent advancements in this emerging area. Each paper submission went through a rigorous peer review process, in addition to multiple follow-up rounds with the authors. A summary of each paper is provided below.

2. Secure communication

Ensuring the integrity and privacy of user data is a crucial component in any technology that involves data outsourcing, cloud computing, and user data. The reality is that this data can potentially be the subject of surveillance and attack [1].

In this mini-track, for example, Gadient [2] investigates control flow integrity to mitigate attacks. Specifically, in this work, the author presents a control-flow attack, and a Counterfeit Object-Oriented Programming (COOP) attack technique, along with other exploits to derive a list of attacker requirements for exploiting a program. From there, the author discusses mitigation techniques that could be effective in these attack scenarios like hardware enforced hash tables, instrumentation that ensures appropriate library calls, and complier changes that force pointers to use read only memory.

Natural discussions elicited from this research include custom hardware the integration of operating systems with hardware components, to the effectiveness of randomization solutions, to moving target solutions in this environment

3. Information security policy compliance

Security, forensic readiness and compliance are elusive topics of interest to both practitioners and academics [3]. In this mini-track, Jeon and Hovav [4] present an employee empowered enterprise management system that is comprised of concepts like psychological ownership, perceived benefit, audit awareness, perceived control and ease of use. Their solution is intended to enhance information security policy compliance.

The authors then compare their solution to a conventional digital rights management system, which is typically composed of hierarchical control based mechanisms. The results highlight the differences between a conventional and an employee empowered approach.

URI: http://hdl.handle.net/10125/50584
ISBN: 978-0-9981331-1-9

4. Location in Air Traffic Networks

The security of air traffic control networks and associated digital forensic issues are increasingly becoming topics of interest in academic environments [6].

The paper presented by Manuel and Li [5] investigates short-term and long term solutions that will provide a secure verification of Automatic Dependent Surveillance-Broadcast (ADS-B) location information that is being transmitted over air traffic control networks. Their short-term solution utilizes a multilateration concept in conjunction with data fusion from redundant systems. Their long-term solutions propose additional software that would reside on top of existing infrastructure. The data would combine existing data like flight plans and ADS-B along with current air traffic control data.

5. Research roadmap

In summary, the papers presented in this mini-track contribute to addressing the knowledge gap between existing scholarship and challenges in the field of cyber-of-things: cyber-crimes and cyber-forensics. However, numerous challenges remain in this emerging research area.

For example, there is an ongoing need to research a) technology investigation efficiency, b) technical integration and solution impact, c) the abuse of technology through cyber-physical attacks along with d) the cost-effective analysis and evaluation of large data repositories. Hence, identifying and validating technical solutions to access data from new technologies, investigating the impact that these solutions have on industry and understanding how technologies can be abused from a cyber-physical perspective are crucial to the viability of government, commercial, and legal communities.

Potential future research would include:

- Research that examines vulnerabilities and solutions to devices that belong to CoT (e.g. CPS, and IoT).;
- Research agendas that identify cyber-crimes, digital forensic issues and resolutions, security vulnerabilities, solutions and approaches to solving complex investigation problems; and
- Research agendas that investigate cost effective retrieval, analysis and evaluation of large data repositories.

References

[1] Devender, Maureen S. Van, William Bradley Glisson, Ryan Benton, and George Grispos, "Understanding De-Identification of Healthcare Big Data", Americas Conference on Information Systems, Boston, 2017

[2] Gadient, Austin J., "On the Effectiveness of Hardware Enforced Control Flow Integrity", ScolarSpace, Hawaii, 2018

[3] Grispos, George, Sorren Hanvey, and Bashar Nuseibeh, "Use of Organisational Topologies for Forensic Investigations", Proceedings of the 1st ACM SIGSOFT International Workshop on Software Engineering and Digital Forensics, 2017, pp. 2-5.

[4] Jeon, Soohyun, and Anat Hovav, "A Novel Method to Enhance Issp Compliant: An Approach Drawing Upon the Concept of Empowerment in Erm System Workflow", ScolarSpace, Hawaii, 2018

[5] Manuel, Nikki, and Depeng Li, "Short-Term and Long-Term Solutions for Secure Verification of Aircraftreported Ads-B Location in Air Traffic Networks", ScolarSpace, Hawaii, 2018

[6] Mink, Dustin, William Bradley Glisson, Ryan Benton, and Kim-Kwang Raymond Choo, "Manipulating the Five V's in the Next Generation Air Transportation System", Springer, Niagara Falls, Canada, 2017