Cybersecurity Investigations and Digital Forensics: Mini-track Overview

William Bradley Glisson
Cyber Forensics
Intelligence Center
Dept. of Computer Science
Sam Houston State University
glisson@shsu.edu

George Grispos
School of
Interdisciplinary Informatics
College of Info. Science & Tech
University of Nebraska-Omaha
ggrispos@unomaha.edu

Kim-Kwang Raymond Choo
Department of Information
Systems and Cyber Security
College of Business
University of Texas-San Antonio
raymond.choo@utsa.edi

Abstract

The continuous amalgamation of technology into everyday life is creating an environment that is conducive to encouraging cybercrimes. As a result, it is becoming increasingly important that organizations and law enforcement agencies have the capability to conduct in-depth and detailed investigations. Hence, corporate and legal responses that address the resulting concerns presented in this mini-track include 'DNA Feature Selection for Discriminating WirelessHART IIoT Devices' and 'Container and VM Visualization for Rapid Forensic Analysis'. These contributions highlight the growing need to investigate and address cyber-security vulnerabilities in the broad context of today's information-driven society.

1. Introduction

As technology is increasingly incorporated into aspects of daily life, cybersecurity and digital forensics investigations need to evolve and diversify [1-9]. This results in the necessity of innovative managerial, technological, and strategic solutions to address resulting concerns [10-13]. This environment presents the opportunity to research a) technology investigations, b) technical integration and solution impact, c) the abuse of technology through attacks along with d) the effective analysis and evaluation of proposed solutions. Identifying and validating technical solutions to access data from new 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.

This mini-track is dedicated to reporting state-of-the-art research in the emerging area of cybersecurity investigations and digital forensics. This year, the mini-track received multiple submissions, of which two were accepted for publication. Each paper went through a rigorous peer-review process, as well as follow-up rounds with the authors. A summary of each paper is provided below.

2. DNA Feature Selection

The proliferation of Wireless Highway Addressable Remote Transducer (WirelessHART) communications in support of Industrial Internet of Things (IIoT) applications are accompanied by increased vulnerability concerns that amplify the need for improved pre-attack security and post-attack forensic methods. In their paper 'DNA Feature Selection for Discriminating WirelessHART IIoT Devices,' Rondeau, Temple, and Kabban [14] investigate activities aimed at applying Time Domain Distinct Native Attribute (TD-DNA) fingerprinting and improving feature selection to increase computational efficiency and the potential for near-real-time operational application. Assessments include both pre-classification and post-classification dimensional reduction using TD-DNA fingerprint features extracted from experimentally collected WirelessHART signals. Results show that pre-classification selection methods are superior, with average percent correct classification differential of 8% $< \%C_{\Delta} <$ 1% being maintained using selected feature subsets containing only 24 (10%) of the 243 full-dimensional features.

3. Container and VM Visualization

Cloud-based and virtualization-centric digital forensic investigations continue to pose problems for forensic investigators. Hence, further socio-technical and technical solutions are needed to provide investigators with the tools and techniques to collect evidence from such environments.

URI: https://hdl.handle.net/10125/64523
978-0-9981331-3-3

In their paper titled 'Container and VM Visualization for Rapid Forensic Analysis,' Shropshire and Benton [15] argue that most cloud security incidents are initially detected by automated monitoring tools. Because they are tuned to minimize the risk of false-negative errors, these tools cast a wide net of suspicion. Depending on the incident scale, the automated tools may implicate rather long lists of virtual machines and containers. Hence, this approach proposes a new intermediate step aimed at reducing the number of virtual machines and containers awaiting forensic investigation. The proposed method renders two-dimensional visualizations of container contents and virtual machine disk images. The visualizations can be used to fingerprint containers, pinpoint instances of embedded malware, and find modified code.

4. Summary

In summary, the papers presented in this mini-track contribute to addressing the knowledge gap between existing scholarship and challenges in the field of cybersecurity investigation and digital forensics. However, a number of challenges remain in this emerging research area that includes but is not limited to technical solutions to cyber-crime, resolution of digital forensic issues, and security vulnerabilities. The challenges include the identification of solutions and approaches to solving complex investigation that involves technology such as smart cities, cyber-physical systems, and internet of things environments. In addition, growing storage capacities warrant further research into retrieval, analysis, and evaluation of large data repositories.

5. References

[1] Grispos, G., W. Glisson, and P. Cooper. *A Bleeding Digital Heart: Identifying Residual Data Generation from Smartphone Applications Interacting with Medical Devices*. in *Proceedings of the 52nd Hawaii International Conference on System Sciences*. 2019. Hawaii, USA.

[2] Grispos, G., W. Glisson, and T. Storer. *How Good is Your Data? Investigating the Quality of Data Generated During Security Incident Response Investigations*. in *Proceedings of the 52nd Hawaii International Conference on System Sciences*. 2019.

[3] Grispos, G., W.B. Glisson, and T. Storer, *Using Smartphones as a Proxy for Forensic Evidence Contained in Cloud Storage Services*, in *46th Hawaii International Conference on System Sciences*. 2013: Hawaii, USA.

[4] Grispos, G., W.B. Glisson, and T. Storer, *Recovering Residual Forensic Data from Smartphone Interactions with Cloud Storage Providers*, in *The Cloud Security Ecosystem*, K.-K.R. Choo and R. Ko, Editors. 2015, Syngress: Boston. p. 347-382.

[5] Grispos, G., W.B. Glisson, and T. Storer, *Enhancing security incident response follow-up efforts with lightweight, agile retrospectives.* Digital Investigation, 2017. **22**: p. 62-73.

[6] Flynn, T., G. Grispos, W.B. Glisson, and W. Mahoney, *Knock! Knock! Who is There? Investigating Data Leakage from a Medical Internet of Things Hijacking Attack*, in *The 53rd Hawaii International Conference on System Sciences (HICSS-53)*. 2020: Maui, HI, USA.

[7] Grispos, G., W.B. Glisson, and K.-K.R. Choo. *Medical cyber-physical systems development: A forensics-driven approach*. in *Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*. 2017. IEEE Press.

[8] Grispos, G., W.B. Glisson, and T. Storer, *Security incident response criteria: A practitioner's perspective*, in *2015 Americas Conference on Information Systems (AMCIS 2015)*. 2015: Puerto Rico, USA.

[9] Grispos, G., J. García-Galán, L. Pasquale, and B. Nuseibeh. *Are you ready? towards the engineering of forensic-ready systems*. in *2017 11th International Conference on Research Challenges in Information Science (RCIS)*. 2017. IEEE.

[10] Grispos, G., *On the enhancement of data quality in security incident response investigations*. 2016, University of Glasgow.

[11] Grispos, G., W.B. Glisson, D. Bourrie, T. Storer, and S. Miller, *Security Incident Recognition and Reporting (SIRR): An Industrial Perspective.* 2017.

[12] Grispos, G., W.B. Glisson, and T. Storer. *Cloud Security Challenges: Investigating Policies, Standards, And Guidelines In A Fortune 500 Organization*. in *21st European Conference on Information Systems*. Utrecht, The Netherlands.

[13] Shetty, R., G. Grispos, and K.-K.R. Choo, *Are you dating danger? an interdisciplinary approach to evaluating the (in) security of android dating apps.* IEEE Transactions on Sustainable Computing, 2017.

[14] Rondeau, C.M., M.A. Temple, and C.S. Kabban. *DNA Feature Selection for Discriminating WirelessHART IIoT Devices*. in *The 53rd Hawaii International Conference on System Sciences (HICSS-53)*. 2020. Maui, HI, USA.

[15] Shropshire, J. and R. Benton. *Container and VM Visualization for Rapid Incident Response*. in *The 53rd Hawaii International Conference on System Sciences (HICSS-53)*. 2020. Maui, HI, USA.