Introduction to the Cyber-of-Things: Cyber-crimes and Cyber-Security Mini-track

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 ever increasing facets of everyday life are conducive to encouraging cyber-crimes and cyber-security evolution and diversification. Hence, responses that address resulting concerns presented in this mini-track include 'A Synchronized Shared Key Generation Method for Maintaining End-to-End Security of Big Data Streams', 'A Threat-Vulnerability Based Risk Analysis Model for Cyber Physical System Security' and an analysis of 'How Espoused Culture Influences Misuse Intention: A Micro-Institutional Theory Perspective'. These contributions highlight the growing need to highlight, investigate and address cyber-security vulnerabilities in the broad context of cyber-of-things.

1. Introduction

As technology is incorporated into more aspects of daily life, cyber-crimes and cyber-security evolve and diversify. This is what some scholars have coined as "cyberization" of everything [16], or Cyber-of-Things (CoT). The changing landscape results in the need to develop innovative managerial, technological and strategic solutions. Increasing mobile device sales; increasing digital evidence requests in legal environments [1, 18, 22, 23]; increasing generation and storage of digital transactions through CoT or Internet-of-Things (IoT) [7, 14]; the applicability of organizational policies, standards and procedures in rapidly evolving environments [6, 8]; and the development of cyber-physical attacks [2, 5, 9, 10, 17], all highlight the broad societal impacts of technology that encourage data intensive environments.

This mini-track is dedicated to reporting the state-of-the-art and recent advancements in this emerging area of enquiry. In the second year for the mini-track, we received 6 submissions, of which only 3 were accepted for publication. The low number of submissions is, perhaps, an indication of the emerging nature of this area. Each paper 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 end-to-end communication

Ensuring the privacy of user data and computations is a crucial component in any technology which involves data outsourcing, cloud computing, and user data. The reality is that this data can potentially be the subject of surveillance [3, 17].

In this mini-track, Puthal, Nepal, Ranjan and Chen [21] highlight the importance of ensuring one of the key problems in big data stream which is ensuring end-to-end security in an Internet of Things (IoT) deployment. Specifically, in this work, the authors present Dynamic Prime Number Based Security Verification (DPBSV) and Dynamic Key Length Based Security Framework (DLSeF) methods that are designed for big data streams based on a shared key derived from synchronized prime numbers in their earlier research.

Natural discussions elicited from this research include the examination of the applicability of forensic frameworks such as the one presented by Rahman, et. al., [24] and the suitability of such solutions to problems that have been highlighted in next generation aircraft architectures [19] and in anti-forensic situations [13].

3. Risk management and mitigation

Risk management is a topic that has been widely studied, although the decentralized architectural and composition of a cyber-physical system (CPS) may

URI: http://hdl.handle.net/10125/41888
ISBN: 978-0-9981331-0-2

require a different risk management and mitigation strategy.

Ledwaba and Venter [15] present a risk model designed for CPS. The authors demonstrate how the risk model can be used in practice. The findings from this work highlight the importance of ensuring that security solution designers are aware of the asymmetric computational nature of components with a CPS deployment. This is an observation echoed by Yang, et. al., [26], who recommend that CPS security solution designers shift from focusing on designing individual lightweight cryptographic primitives to taking a whole-of-system approach to achieve (1) system/collective lightweightness, (2) outsource expensive computations from resource-constrained field devices to neighboring devices and equipment that have more computational capacity, and (3) selectively protect critical data (partial/selective protection of Data of Interest). As Yampolskiy, et. al, [25] note these types of issues become paramount when considering the protection of intellectual property in conjunction with practical outsourcing solutions.

4. Effect of culture on system misuse

In addition to technological solutions described in the other two papers of this mini-track, it is important to reinforce security awareness at the individual / user level, as well as to understand the effect of espoused institutional pressure at an organizational level. Previous work highlights the fact that employees do not always follow organizational policies, standards and procedures [6] and that polices and systems need to evolve as technology advances [8, 11].

Hovav [12] presents the results of their work where they used micro-institutional pressures, namely: coercive, normative and mimetic, to examine motivators and inhibitors of information system misuse in South Korea. Based on the analysis of 232 usable survey responses, the author suggested that normative pressure is generally more effective than the use of sanctions in an Asian culture, and recommended that organizations cultivate a proactive management environment to maximize cyber security compliance.

5. Potential research roadmap

In summary, the papers presented in this mini-track contribute to filling the knowledge gap between existing scholarship and challenges in the field of cyber-of-things: cyber-crimes and cyber-security. However, there remains a number of challenges to be addressed 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 agendas that investigate vulnerabilities and solutions to devices that belong to CoT (e.g. CPS, and IoT) [1];
- 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] Berman, K., W. B. Glisson, and L. M. Glisson, "Investigating the Impact of Global Positioning System (Gps) Evidence in Court Cases", Hawaii International Conference on System Sciences (HICSS-48), 2015

[2] Cahyani, N. D. W., B. Martini, K.-K. R. Choo, and A. M. N. Al-Azhar, "Forensic Data Acquisition from Cloud-of-Things Devices: Windows Smartphones as a Case Study", Concurrency and Computation: Practice and Experience, 2016, pp. n/a-n/a.

[3] Choo, K. K. R., and R. Sarre, "Balancing Privacy with Legitimate Surveillance and Lawful Data Access", IEEE Cloud Computing, 2(4), 2015, pp. 8-13.

[1] For example, two recent studies [4, 20] pointed out the importance of ensuring security in the design of CoT systems such as three dimensional (3D) printers. The studies demonstrated how an attacker can exploit vulnerabilities in these devices to exfiltrate previously printed and current model files; consequently, causing significant intellectual property damage and/or financial harm to an organization who is manufacturing product prototypes on these printers

[4] Do, Q., B. Martini, and K. K. R. Choo, "A Data Exfiltration and Remote Exploitation Attack on Consumer 3d Printers", IEEE Transactions on Information Forensics and Security, 11(10), 2016, pp. 2174-2186.

[5] Dorazio, C. J., K. K. R. Choo, and L. T. Yang, "Data Exfiltration from Internet of Things Devices: Ios Devices as Case Studies", IEEE Internet of Things Journal, PP(99), 2016, pp. 1-1.

[6] Glisson, W. B., and T. Storer, "Investigating Information Security Risks of Mobile Device Use within Organizations ", Americas Conference on Information Systems (AMCIS), 2013

[7] Glisson, W. B., T. Andel, T. Mcdonald, M. Jacobs, M. Campbel, and J. Mayr, "Compromising a Medical Mannequin", Americas Conference on Information Systems (AMCIS), 2015

[8] Grispos, G., W. B. Glisson, and T. Storer, "Cloud Security Challenges: Investigating Policies, Standards and Guidelinges in a Fortune 500 Organization", Utrecht University, 2013

[9] Grispos, G., W. B. Glisson, J. H. Pardue, and M. Dickson, "Identifying User Behavior from Residual Data in Cloud-Based Synchronized Apps", Journal of Information Systems Applied Research, 8(2), 2015, pp. 4-14.

[10] Grispos, G., W. B. Glisson, and T. Storer, "Chapter 16 - Recovering Residual Forensic Data from Smartphone Interactions with Cloud Storage Providers", in (Choo, R.K.-K.R., 'ed.' The Cloud Security Ecosystem, Syngress, Boston, 2015, pp. 347-382.

[11] Hoolachan, S., and W. B. Glisson, "Organizational Handling of Digital Evidence", Association of Digital Forensics, Security and Law, St. Paul, Minnesota, USA, 2010

[12] Hovav, A., "How Espoused Culture Influences Misuse Intention: A Micro-Institutional Theory Perspective", Hawaii International Conference on System Sciences (HICSS-50), 2017

[13] Karlsson, K.-J., and W. B. Glisson, "Android Anti-Forensics: Modifying Cyanogenmod", Hawaii International Conference on System Sciences (HICSS-47), 2014

[14] Kynigos, C., W. B. Glisson, T. R. Andel, and J. T. Mcdonald, "Utilizing the Cloud to Store Camera-Hijacked Images ", Hawaii International Conference on System Sciences (HICSS-49), 2016

[15] Ledwaba, L., and H. S. Venter, "A Threat-Vulnerability Based Risk Analysis Model for Cyber Physical System Security", Hawaii International Conference on System Sciences (HICSS-50), 2017

[16] Ma, J., K.-K. R. Choo, H.-H. Hsu, W. L. Q. Jin, Y. W. K. Wang, and X. Zhou, "Perspectives on Cyber Science and Technology for Cyberization and Cyber-Enabled Worlds", Cyber Science and Technology Congress (CyberSciTech), 2016

[17] Mckeown, S., D. Maxwell, L. Azzopardi, and W. B. Glisson, "Investigating People: A Qualitative Analysis of the Search Behaviours of Open-Source Intelligence Analysts", The 5th Information Interaction in Context Conference (IIiX), 2014

[18] Mcmillan, J., W. B. Glisson, and M. Bromby, "Investigating the Increase in Mobile Phone Evidence in Criminal Activities", Hawaii International Conference on System Sciences (HICSS-46), 2013

[19] Mink, D., A. Yasinsac, K. K. R. Choo, and W. Glisson, "Next Generation Aircraft Architecture and Digital Forensic", AMCIS, San Diego, California, 2016

[20] Moore, S. B., W. B. Glisson, and M. Yampolskiy, "Implications of Malicious 3d Printer Firmware", Hawaii International Conference on System Sciences (HICSS-50), 2017

[21] Puthal, D., S. Nepal, R. Ranjan, and J. Chen, "A Synchronized Shared Key Generation Method for Maintaining End-to-End Security of Big Data Streams", Hawaii International Conference on System Sciences (HICSS-50), 2017

[22] Quick, D., B. Martini, and R. Choo, Cloud Storage Forensics, Syngress Publishing / Elsevier, Waltham, MA, 2013.

[23] Quick, D., and K.-K. R. Choo, "Big Forensic Data Reduction: Digital Forensic Images and Electronic Evidence", Cluster Computing, 19(2), 2016, pp. 723-740.

[24] Rahman, N. H. A., W. B. Glisson, Y. Yang, and K. K. R. Choo, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems", IEEE Cloud Computing, 3(1), 2016, pp. 50-59.

[25] Yampolskiy, M., W. B. Glisson, and A. Yasinsac, "Intellectual Property Protection in Additive Layer Manufacturing: Requirements for Secure Outsourcing", 4th Program Protection and Reverse Engineering Workshop (PPREW), 2014

[26] Yang, Y., J. Lu, K.-K. R. Choo, and J. K. Liu, "On Lightweight Security Enforcement in Cyber-Physical Systems", in (Güneysu, T., Leander, G., and Moradi, A., 'eds.'): Lightweight Cryptography for Security and Privacy: 4th International Workshop, Lightsec 2015, Bochum, Germany, September 10–11, 2015, Revised Selected Papers, Springer International Publishing, Cham, 2016, pp. 97-112.