CYPHYS: Cyber-Physical Security

The Tenth International Conference on Advances in Circuits, Electronics and Micro-electronics
(CENICS 2017: http://www.iaria.org/conferences2017/CENICS17.html)

Alie El-Din Mady
United Technologies Research Center
Cork Ireland
Madyaa@utrc.utc.com

***Abstract*— Given the recent increase in frequency, sophistication and success of cyber-attacks against Cyber Physical System (CPS) infrastructure, such as nuclear reactor, the urgent need for advanced cyber physical security solutions is clearly evident. Typical cyber security protection mechanisms are no longer a full guarantee for the CPS security, due to the vulnerabilities introduced at the integration boundary between cyber and physical systems. CYPHYS special track is calling researchers to look for developing novel CPS security solutions. In CYPHYS, we focus on the following directions in CPS security: i) how can the physical system add a value to the legacy cyber security technology, ii) designing cyber security solutions taking in account the physical environment under control and iii) hardening the CPS security.**

Keywords-Cyber-physical systems; Intrusion detection; Cybersecurity

I. Introduction

Cyber-Physical System (CPS) tightly integrates physical environment with hardware and software elements and as a result identifying whether behavioral attributes are consequence of computations, physical laws, or both working together is challenging. CPS has been at the core of critical infrastructures and industrial systems, such as power and water, transportation systems, medical devices, security systems, building automation and emergency management. There have been many confirmed cases of cyber-attacks within CPS, such as The StuxNet cyberattack targeting a nuclear-enrichment plant in Iran [1], and BlackEnergy malware targeting several electricity distribution companies in Ukraine [2]. These systems are becoming more vulnerable to cyber-attacks due to the wide attack vector resulted from the integration complexity increase. Cybersecurity threats exploit the increased complexity and connectivity of critical CPS based on Internet of Things (IoT), such as, placing the Nation's security, economy, public safety, and health at risk. Typically, the interfaces between hardware components, between hardware and software components, and between software components, as well as between a system and its operators and maintainers, have been sources of vulnerability. When a CPS is attacked, the operation of the corresponding system can lead to physical safety, trigger loss of life, cause enormous economic impact, and thwart the vital missions of businesses, cities, states and the nation. The goal of CYPHYS special track is to foster novel, transformative and multidisciplinary approaches that ensure the security of current and emerging cyber-physical systems, called Cyber-Physical Security, by taking into consideration the unique challenges present in this environment. This special track also aims to foster a research community committed to advancing research and education at the confluence of cybersecurity, internet of things, and cyber-physical systems, and to transitioning its findings into engineering practice.

The CYPHYS track includes the following topics:

1. Embedded systems security
2. PUFs/Watermarking
3. Trustworthy devices and CPS
4. Hardware-based intrusion detection
5. Intrusion detection for CPS
6. Resiliency and adaptive attack mitigation for CPS
7. Security policies and dynamic enforcement for CPS/IoT
8. CPS vulnerability analysis
9. Device and CPS hardening
10. Threat modelling for CPS

II. Submissions

The total number of submissions are four papers [3][4][5][6]. Out of these papers, there are three papers [3][4][5] have discussed the anomaly-based detection technology in the context of CPS security. The papers have proven that anomaly-based intrusion detection is effective when it is applied in CPS security. The effectiveness of the method is introduced from the use of physical model to identify any malicious behavior introduced through the cyber system.

The first paper [3] is titled "*Towards an Implementation of Data Analytics for Smart Grid Security*". This paper presents a security information analytics framework, using various data analytics methods to detect anomalies in metered data that may indicate attacks. The implementation of the framework has been applied to a live micro-grid test-bed for the modeling of normal behavior and for performance analysis. Furthermore, the framework is scalable, allowing additional analysis tools and resilient control solutions to be incorporated, further enhancing the reliability of the system.

The second paper [4] is tilted “*Anomaly-Based Intrusion Detection System for Embedded Devices on Internet*”. This paper proposes an Intrusion Detection and Resilient Policy methodology for embedded devices connected to the Internet. It summarized various attack models for Internet connected embedded systems.

The third paper [5] is titled “*Physics-Based Methods for Distinguishing Attacks from Faults*”. This article uses physics-based methods for distinguishing attacks from faults. It frames a CPS as a discrete-time linear system that can switch between various modes. By encoding faults and attacks each as specific modes, it builds CPS models that incorporate the impact of a range of types of fault and attack. It then uses this CPS model to isolate (and distinguish between) a fault and an attack.

Finally, paper [6] titled “*Towards Secure Building Management System based on Internet of Things*” proposes a holistic overview of designing a secure framework for Internet of Things (IoT) system, where the framework will be implemented as part of an ongoing H2020 project called ANASTACIA: Advanced Networked Agents for Security and Trust Assessment in Cyber-Physical System (CPS) based on IoT Architectures. The paper considers Energy management system for building automation as an application for CPS based IoT.

III. Conclusion

The CYPHYS special session includes a broad range of topics related to cyber physical security. It contains both solid research and future EU plans/studies. The need for the CPS security has been demonstrated clearly by all papers. In addition, anomaly-based intrusion detection has been discussed by several papers as a promising approach to go forward towards intrusion detection for CPS systems.

References

[1] J. P. Farwell and R. Rohozinski, “Stuxnet and the future of cyber war,” Survival Journal, vol. 53, 2011, pp. 23–40.

[2] Available. Blackenergy. [Online]: http://www.securityweek.com/blackenergy-group-uses-destructiveplugin-ukraine-attacks (2015)

[3] Jacobo Blanco, Silvio La Porta, Niamh O’Mahony, Rohan Chabukswar, Alie El-Din Mady and Menouer Boubekeur, Towards an Implementation of Data Analytics for Smart Grid Security, CENICS 2017, The Tenth International Conference on Advances in Circuits, Electronics and Micro-electronics, September 10 - 14, 2017 - Rome, Italy, www.thinkmind.org

[4] Deepak Mehta, Alie El-Din Mady, and Menouer Boubekeur, Devu Manikantan Shila, Anomaly-Based Intrusion Detection System for Embedded Devices on Internet, CENICS 2017, The Tenth International Conference on Advances in Circuits, Electronics and Micro-electronics, September 10 - 14, 2017 - Rome, Italy, www.thinkmind.org

[5] Gregory Provan Riccardo Orizio, Physics-Based Methods for Distinguishing Attacks from Faults, CENICS 2017, The Tenth International Conference on Advances in Circuits, Electronics and Micro-electronics, September 10 - 14, 2017 - Rome, Italy, www.thinkmind.org

[6] Alie El-din Mady, Ruben Traperoy, Antonio Skarmetaz and Stefano Bianchi, Towards Secure Building Management System based on Internet of Things, CENICS 2017, The Tenth International Conference on Advances in Circuits, Electronics and Micro-electronics, September 10 - 14, 2017 - Rome, Italy, www.thinkmind.org