International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

Upsurging Cyber-Kinetic attacks in Mobile Cyber Physical Systems

Gifty R[1], Bharathi R[2]

[1]Ph.D, Department of Information and Communication Engineering, Anna University Nagercoil, TN, India.
[2]Assistant professor and Head of the Department of Electronics and communication, University college of Engineering, Nagercoil, Tn-India.

Abstract – *Securing critical infrastructures which are Cyber Physical Systems (CPS) such as HealthCare, Banking, and Water Systems from intense cyber threats is crucial. The CPS design process follows a Mathematical Model for physics based systems and a Control theoretic model for the control system. But while modeling a secure CPS system, the design approach is set by stepping into the shoes of a malicious attacker. In this paper, we consider some of these cyber threats and discuss the techniques and methodologies for defending CPS systems. We summarize different approaches that are capable of identifying Cyber threats at different levels of design process and also add practical procedures that can be utilized to design secure CPS Systems.*

Index Terms – Cyber Physical Systems (CPS), Cyber threats, control system, Data security, Privacy models*.*

1 INTRODUCTION

CPS include cyber capability i.e. networking and computational capability in every physical component; they are networked at multiple and extreme scales. Research advances in cyber-physical systems promise to transform our world with systems that respond and work in dangerous or inaccessible environments precisely. Autonomous collision avoidance, robotic surgery and nano-tolerance manufacturing, assistive technologies and ubiquitous healthcare monitoring and delivery are the extended applications of CPS.

Attacks on CPS interrupt the services and lead to severe disaster. It is essential to ensure that the CPS is secure for all cyber and physical services. CPS HealthCare systems monitor a patient through body worn inexpensive personal monitoring devices that record multiple physiological signals, such as ECG and heart rate[1],[2], or more sophisticated devices that measure physiological markers such as body temperature, skin resistance, gait, posture, and EMG [3], [4]. The medical data that is acquired from patients by a distributed sensor network can be transmitted to private [9], [10] or public [11]–[13] cloud services. Assuring the privacy of the personal information during the transmission from the sensory networks to the cloud and from the cloud to mobile devices will necessitate the design of a sophisticated cryptographic architecture for a CPS. While this design implies only secure storage using conventional encryption schemes, emerging encryption schemes provide options for secure data sharing and secure computation[5].

This paper is organized as follows: In Section II, we survey the literature by summarizing few security approaches and threats. Section III portrays the security modeling and optimization in CPS. Section IV reviews the security and privacy models in CPS applications. Section V demonstrates the model verification and synthesis, and analyses the result with existing models.

2 REVIEW OF PERTINENT STUDIES

Ensuring security is increasingly challenging in cyber-physical systems, where information security methods such as key management, secure communication, and code execution may guarantee the integrity of the cyber components and data, but are ineffective against insider and physical attacks. Some of the core hardware and protocols adopted in cyber-physical systems are of public domain, thus vulnerable to cyber and physical attacks.

Fabio Pasqualetti et al (2015) [17] portray a simplified framework for the design and operation of secure cyber-physical systems based on control theory, information security, and embedded system design. This framework relies on informative mathematical models for various system objectives, including control performance, system security, and platform schedulability, and it quantifies their interdependency by means of a minimal set of interface variables and relations.

Data management in CPS provides the approach to manage the collected data to satisfy the user requirement. Data need to be integrated and stored from multiple sensors for future use. Processing the data provides better information accumulation and communication. Sensed data may not be usable in raw format as this requires large bandwidth and efficient processing. Some other characteristics of data management process should be real-time data processing and routing, reliable event detection, security, and robustness.

Wenjia Li et al (2013) [20] studied a trustworthy data management framework for CPS, which is called Real Alert. In this framework, the trustworthiness of the data as well as the reporting sensors are computed based on both the abnormal sensor data and multiple contextual conditions in which the abnormal sensor data are observed. Data management process consists of three elements: (a) data integration, (b) data storage, and (c) data processing.

Data integration provides the service of data gathering from distributed sensors for obtaining better knowledge. This also decreases the amount of data required to transmit. Data integration process can be divided in two elements, such as combined and individual. In combined data integration, data collected from multiple sensors can be integrated for further processing. The wide range of data from individual sensors are collected and integrated in individual data integration.

Data Storage: The data in the real-time database must be able to provide information about the present state of the system they represent, especially when the application area is critical such as a patient care system. Two main approaches to storage and querying data are generally considered; they are warehousing (central) and distributed. The warehousing approach stores data in a central database and then queries may be performed to it. In a distributed approach, sensor devices are considered as local databases and data are managed locally.

Data Processing: For efficient computation and communication, the data need to be processed properly. Data processing can be performed in distributed manner, in based station or in cloud. The data processing decision has to be made according to the application and available resources. The timely access and processing of sensed data from sensors are critical for CPS.

3 MODELING AND OPTIMIZATION OF CPS

Computations in CPS for healthcare are performed for two elements: (a) modeling and (b) monitoring. Cloud Computing can perform large-scale and complex computation and communication so that data by sensors can be easily collect from remote observation centers. Designing cyber-physical system requires vast computation due to the involvement of large network and environment. The environment often involves multiple domains such as control, communication, feedback, and response. To validate the design, model based computations are performed.

Model-Based Design (MBD) has been identified as a powerful design technique for CPSs. Specifications of system and its underlying components are defined in the form of models able to reflect the evolution of the system. These models can be used for early design analysis. Jeff C. Jensen et al [21] have decomposed model-based design into a set of sequential steps that, describe and evaluate an iterative design methodology, and evaluate this methodology in the development of a cyber-physical system. By making use of models, it is possible to have earlier identification of design defects instead of during the prototyping.

Platform-Based Design (PBD) methodology consists of two main steps, namely, system architecture design and control design. The system architecture design step instantiates system components and interconnections among them to generate an optimal architecture while guaranteeing the desired performance, safety, and reliability. The embedded system architecture consists of software, hardware, and communication components, while the plant architecture depends on the physical system under control, and may consist of mechanical, electrical, hydraulic, or thermal components. Nuzzo et al [22] formalized the above design concepts and enable the realization of system architectures and control algorithms in a hierarchical and compositional manner that satisfies the constraints and optimizes the function.

Contract-Based Design (CBD) has many benefits: reuse, clean interfaces, separation of concerns, etc. Alberto Sangiovanni et al [23] stated that contract-based design must be developed by considering the following: (i) Mathematical foundations for contract representation that enable the design of frameworks and tools; (ii) A system framework and associated methodologies that focus on system requirement modeling, contract specification, and verification at multiple abstraction layers; (iii) framework focusing on cross boundary design flows that addresses impacts of CBD.

4 DATA SECURITY AND PRIVACY MODELS FOR CPS

Security is a vital concern here as data is confidential from legal and ethical perspectives. While designing CPS architecture for applications, special attention needs to be paid to ensure data security. Security has two components: (a) privacy and (b) encryption. Privacy: Ensuring data privacy is an important issue from application level and data level. Data encryption can be a solution for security assurance. Security models can be useful for estimating risk and other security metrics.

Edward Colbert et al (2017) [27] stated that there are five well known classes of methods for cyber risk assessment and management for CPS. An Expert Elicited Model method involves computational models to assess risk based on expert elicited identification and characterization of cyber system attributes such as network data flows and the estimation of the susceptibility of those resources and data flows to different types of compromise. This approach possesses significant appeal for many applications, including cases involving complicated networks for which little design information is readily available and cases in which a relatively quick analysis is needed. One major drawback of this approach is lack of completeness.

Second, the Attack Graph method advocates construction of attack trees or graphs, either by hand or through automated interrogation of a system of interest. This approach has many advantages. Principal among these is a very light data requirement. Models in this class do not suffer precision or fidelity shortcomings because they are constructed directly from system data without abstraction or aggregation. Another advantage of this approach is flexibility.

Third, game theoretic models explicitly account for the interaction of attackers and defenders in a game theoretic framework. Models in this class are much more varied, and the approach is much less mature than the expert elicited and graph-based approaches described previously. Games can inform how the playing field can be better tilted in favor of the defender by adopting architectural changes and new access control policies.

The fourth method is Petri Net models, which are favored by the authors of this chapter. This chapter's Petri net approach is derived from the Attack Graph school of thought. A Petri net is a directed bipartite graph, in which a cyber-attack is modeled as the successive exploitation of vulnerabilities on hosts to escalate and then exploit privileges on the network.

The final method described involves stochastic games overlaid on Petri nets, creating a much more powerful, and more challenging, approach. In this model, transitions based on attacks corresponding to network defense measures replace exploit-specific transitions.

5 MODEL CHECKING AND SYNTHESIS FOR CPS

To detect and eliminate design flaws and inevitable bugs are notoriously difficult tasks due to the complex interactions between the cyber and physical components. The synthesizer and runtime system will be responsible for allocating redundant resources, replicating tasks, mapping the application tasks and managing system resources, and coordinating the execution to ensure that 1) scheduling is feasible under realistic processor performance, and 2) the reliability of implementation under realistic resource failures meets the reliability requirement set by the developer.

To verify the correctness of CPS with aggregate effects, model checking on CPS properties are used. This method checks if the CPS model satisfies the specified property. Model Checking for CPS uses Reachability analysis technique to see if the specified property holds for all system states. Automated techniques can be used for CPS model checking.

5.1 Reachability analysis

Reachability analysis is the process of computing the set of reachable states for a system. In order to estimate the aggregate effects in CPS accurately, the nonlinear nature of the system interactions should be considered in that analysis. A major component of a safety verification algorithm for a hybrid system is an efficient method to compute its reachable set, which is the set of all the states visited by all the possible trajectories. The computation of reachable sets by discrete dynamics mainly requires Boolean operations over sets such as intersection of the reachable set with the guard sets of the transitions to determine the trajectories that can switch to a different mode. Computing the set of states reachable by continuous dynamics requires handling sets of solutions of differential or difference equations, and this problem is difficult. For general non-linear equations, their closed form solutions are not known; and even for linear systems the solutions of which can be written in a closed form, their manipulation is difficult because they can contain exponential functions. Therefore, the reachability problem for continuous systems has been a major obstacle towards applying hybrid systems formal verification to real-life problems. This has motivated much research in hybrid systems verification to focus on this particular problem.

B. Controller synthesis

Controller synthesis addresses the question of how to limit the internal behavior of a given implementation to meet its specification, regardless of the behavior enforced by the environment. In system design, the general goal is to develop systems that satisfy user requirement specifications. To simplify this development process, it should be automated and the system should be synthesized based on the requirements.

In such a framework, the plant acts usually in an environment. The goal is to find a schedule for the controllable events that guarantees the specification to be satisfied considering all possible environmental behaviors. One can also understand the controller and environment as two players. The plant constitutes to the game board and controller synthesis becomes the problem of finding a strategy for the controller that satisfies the specification whatever move the environment does, or in other words, under any adversary. The requirement specification can either be given internally or externally. Internal specifications impose restrictions for example on the number of visits of a state of the plant. Examples for external specifications are temporal logic formulas that are supposed to be satisfied by the controlled plant.

C. Vulnerability analysis

With unprotected or inadequately protected devices, communication between sensors, monitoring devices and actuators is vulnerable. Hackers could either introduce false data to trick actuators into taking detrimental actions, or actually take control of the system and command a disruptive event.

According to [3], the vulnerabilities in CPS derive from defects, misconfigurations, CPS network mismanagement or network connectivity with others. These vulnerabilities can be eliminated or reduced through a variety of security controls, such as network design defense, defense in depth, network traffic encryption, network link limit, physical access control on network components.

6 CONCLUSION

The design of security for cyber-physical systems must take into account several characteristics common to such systems. Among these are interactions between the cyber and physical environment, distributed management and control, real-time requirements, and geographic distribution. In this paper, first, we have surveyed conventional and emerging encryption schemes that can be used in designing a CPS. Second, we provided an extensive evaluation of these schemes and compare them based on their ability to provide secure storage, secure data sharing, and secure computation.

References

[1] Fit Bit Inc., "flex: Wireless activity + sleep wristband," accessed April 2015. [Online]. Available: https://www.fitbit.com/flex

[2] Apple Inc., "Apple watch," accessed April 2015. [Online]. Available: https://www.apple.com/watch/

[3] S. X. et al., "Soft microfluidic assemblies of sensors, circuits, and radios for the skin," Science, vol. 344, pp. 70–74, 2014.

[4] D. Kim, R. Ghaffari, N. Lu, and J. A. Rogers, "Flexible and stretchable electronics for bio integrated devices," Annual Review of Biomedical Engineering, pp. 113–128, 2012.

[5] Ovunc Kocabas, et al "Emerging Security Mechanisms for Medical Cyber Physical Systems", IEEE/ACM Transactions on Computational Biology and Bioinformatics, DOI 10.1109/TCBB.2016.2520933

[6] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis, "IEEE Trans. Sys., Man, and Cybernetics, Part C: Applic. and Reviews, vol. 40, no. 1, pp. 1–12, Jan 2010.

[7] A. Page, O. Kocabas, T. Soyata, M. K. Aktas, and J. Couderc, "Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance," Annals of Noninvasive Electrocardiology (ANEC), vol. 20, no. 4, pp. 328–337, 2014.

[8] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. K. Aktas, G. Mateos, B. Kantarci, and S. Andreescu, "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges," in IEEE Int. Conference on Services Computing, Jun 2015, pp. 285–292.

[9] Care Cloud, http://www.carecloud.com/, 2013.

[10] Dr Chrono, https://drchrono.com/, 2013.

[11] "Amazon Web Services," http://aws.amazon.com.

[12] "Google Cloud Platform," https://cloud.google.com/.

[13] "Microsoft Windows Azure," http://www.microsoft.com/windowazure.

[14] C. Neuman, "Challenges in security for cyber-physical systems."

[15] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water scada systems part i: analysis and experimentation of stealthy deception attacks," Control Systems Technology, IEEE Transactions on, vol. 21, no. 5, pp. 1963–1970, 2013.

[16] Sun, Meng. "Challenges on Coordination for Cyber-Physical Systems."Applied Mechanics and Materials. Vol. 347. 2013.

[17] Fabio Pasqualetti, "Design and Operation of Secure Cyber-Physical Systems", IEEE Embedded Systems Letters, Vol 7, Issue 1, pg 3-6, 2015, 10.1109/LES.2014.2367100.

[18] Elias, "A Brief Survey of Security Approaches for Cyber-Physical Systems", IEEE 8th IFIP International Conference on New Technologies, Mobility and Security, pg 1-5, 10.1109/NTMS.2016.7792424.

[19] Siddharth, "Cyber-Physical System Security for the Electric Power Grid", Proceeding of the IEEE, vol 100, Issue 1, 2012,

[20] Fabio Pasqualetti, "Attack Detection and identification in Cyber Physical Systems", IEEE Transactions on Automatic Control, Vol 58, Issue 11, pg 2715-2729, 10.1109/TAC.2013.2266831.

[21] http://indiatoday.intoday.in/ story/ petya-ransom ware- major- global -cyber- attack- wannacry - jawaharlal- nehru-port- trust/ 1/988915.html

[22] http://www.telegraph.co.uk/ technology/ 2016/12/20/hackers- could-take-control-plane-using-in-flight-entertainment/

[23] Rober Mitchell, "Effect of intrusion Detection and Response on Reliability of Cyber Physical Systems", IEEE Transactions on Reliability, Vol 62, Issue 1, pg 199-210, 2013, 10.1109/ TR.2013.2240891.

[24] Robert Eastman, —Big Data and Predictive Analytics: On the Cyber security Front Line‖, IDC Whitepaper, February 2015.

[25] Peng Cheng, "Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop", pg 133-145.

[26] K. Wang and S. Stolfo. Anomalous payload-based network intrusion detection. In Recent Advances in Intrusion Detection, pages 203–222, Sophia Ant polis, 2004.

[27] C. Taylor and J. Alves-Foss. NATE: Network analysis of anomalous traffic events, a low-cost approach. In Proceedings of Workshop on New Security Paradigms, pages 89–96, Cloudcroft, NM, 2001.

[28] R. Mitchell and R. Chen. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 44(5):593–604, 2014.