COMPUTERS & SECURITY 68 (2017) 81–97

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Cyber physical systems security: Analysis, challenges and solutions

Yosef Ashibani *, *Qusay H. Mahmoud*

Department of Electrical, Computer and Software Engineering, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada

ARTICLE INFO

Article history:
Received 28 October 2016
Received in revised form 5 April 2017
Accepted 7 April 2017
Available online 12 April 2017

Keywords:
Cyber Physical Systems (CPS)
Internet of Things (IoT)
CPS security analysis
Risk assessment
Security architecture
Research challenges

ABSTRACT

Cyber Physical Systems (CPS) are networked systems of cyber (computation and communication) and physical (sensors and actuators) components that interact in a feedback loop with the possible help of human intervention, interaction and utilization. These systems will empower our critical infrastructure and have the potential to significantly impact our daily lives as they form the basis for emerging and future smart services. On the other hand, the increased use of CPS brings more threats that could have major consequences for users. Security problems in this area have become a global issue, thus, designing robust, secure and efficient CPS is an active area of research. Security issues are not new, but advances in technology make it necessary to develop new approaches to protect data against undesired consequences. New threats will continue to be exploited and cyber-attacks will continue to emerge, hence the need for new methods to protect CPS. This paper presents an analysis of the security issues at the various layers of CPS architecture, risk assessment and techniques for securing CPS. Finally, challenges, areas for future research and possible solutions are presented and discussed.

1. Introduction

Cyber physical systems (CPS) are a combination of closely integrated physical processes, networking and computation. The physical process is monitored and controlled by embedded (cyber) subsystems via networked systems with feedback loops to change their behavior when needed (Asare et al., 2012). These subsystems work independently of each other with the ability to interact with the external environment (Ali et al., 2015; Wang et al., 2010). The physical processes are achieved by several tiny devices with sensing, computing and communication (often wireless) capabilities. These physical devices can be identified with physical attributes or information sensing equipment, such as infrared sensors or Radio Frequency Identification (RFID), and can then be connected to a networking system, in most cases the Internet, to send the captured data to the computational subsystem (Zhang et al., 2011).

With the increased focus on data handling capacity, data communications capability and integration of information systems, as well as physical devices, the demand for integrating CPS in different fields is also increasing, resulting in widely gained attention not only from universities and research and development labs but also from industry and government agencies (Lu et al., 2015). Prior to the current form, CPS evolved through different stages: Embedded Systems, Intelligent Embedded Systems and Systems of Systems (Sendler, 2013). The

* *Corresponding author.*
E-mail addresses: yosef.ashibani@uoit.net (Y. Ashibani), qusay.mahmoud@uoit.net (Q.H. Mahmoud).
http://dx.doi.org/10.1016/j.cose.2017.04.005
0167-4048/

current form of CPS is used in many different areas such as the power, petroleum, water industry, chemical engineering, healthcare, manufacturing, transportation, automotive systems, entertainment, consumer appliances, in addition to many other areas that are directly related to people's daily lives. It was estimated that cyber physical components would account for 40% of an automobile's total value by the end of 2015 (NIST, 2012), and that in 2020, around 25 billion uniquely identified objects will be used (Jing et al., 2014).

CPS have many features, such as enabling individual components to work jointly, producing complex systems (Vegh and Miclea, 2014). In CPS, data can be captured by physical objects or sensor devices, and transferred through networks to the control system with the absence, in some cases, of any human to machine interaction (Bhabad and Scholar, 2015). The physical objects are increasingly equipped with, for example, infrared sensors, barcodes or RFID tags which can be scanned by smart devices (Khan et al., 2012). These devices can be connected to the Internet to send the identified data and location placement to be used for monitoring and managing the physical environment (Zhang et al., 2011). The computational and processing units can also be placed in the cloud, with the resulting decisions issued as actions to the physical objects (Khan et al., 2012). As an example of CPS, Industrial Control Systems (ICS) are isolated by communication protocols and operating systems from the outer systems. For the time being, these kinds of systems are increasingly interrelated through the Internet in improving functionality and automation. The increased connectivity of the cyber and physical world brings significant security challenges to the CPS (Shafi, 2012). As the importance of these systems is in improving functionality, the interconnectivity among CPS subsystems is growing (Peng et al., 2013).

Security concerns ranging from application environment and communication technology should be addressed at the early stages of the design (Gamundani, 2015). Moreover, the inherent characteristics and advantages of using available networks, such as Wireless Sensor Networks (WSN), Next-Generation Networks and the Internet, CPS are increasingly facing new security challenges, such as securing protocols and establishing trust between CPS subsystems (Lu et al., 2013). Many of the computing subsystems in CPS are based on commercial-off-the-shelf (COTS) components. The COTS components provide a significant level of control, lower deployment, and lower operational costs in comparison to the traditional vendor specific proprietary and closed-source systems. However, this exposes CPS to more vulnerabilities and threats (Nourian and Madnick, 2014). As an example, industrial control systems have been considered secure when not connected to the outside world (Nourian and Madnick, 2014), without taking into account insider attacks. Thus, this indicates that the extensive connectivity between cyber and physical components raises the important issue of security.

More attacks are expected as many interactions among different components are connected outside of their area to provide better services, such as Smart Grid networks. For example, in the field of the power industry, a power plant monitoring system was attacked in 2010. Consequently, a 900MW load was lost in under 7 seconds. In the energy sector, the Iran Bushehr Nuclear Power Plant computer system was attacked by "Stuxnet" in the same year, which led to severe disorder in the nuclear facilities' automated operations and a serious deterioration in Iran's nuclear program (Peng et al., 2013). According to a CIA report, power systems in several regions outside the United States have been penetrated by attackers, leading to power outage in multiple cities. In the medical field, implanted human medical devices have been attacked by hackers through their wireless communications (Leavitt, 2010).

In the transportation field, an exception in the management system of Japan's control schedule resulted in five Shinkansen operation management system failures. Consequently, 124 trains were delayed while 15 trains were suspended, affecting the travel of 8.12 million people (Peng et al., 2013). It has been demonstrated that airplanes could be controlled by attackers via accessing built-in Wi-Fi services (Nourian and Madnick, 2014). In 2010, CarShark was invented, a software with the ability to remotely turn off a car's engine and brakes leading to a loss of control to stop the car. This software was also able to monitor communications between electronic units, providing incorrect readings, and inputting false data to perform the attack. Meanwhile, in that same year, other attackers succeeded in creating a new virus to attack the Siemens plant control system (Wang et al., 2010).

These security incidents provide enough evidence that attacks on CPS, in particular on the cyber layer, can lead to a great loss in people's livelihoods. Therefore, CPS security is becoming more important than ever and should be taken into consideration in the early stage of the design process. Moreover, advanced CPS security techniques are needed to increase the protection of these increasingly complex interconnected systems (Jalali, 2009). Most of the efforts in security solutions were based on the available solutions designed specifically for classical Information Technology (IT) systems to develop or create advanced solutions. However, these solutions are not designed for CPS (Konstantinou et al., 2015; Wang et al., 2010). Additionally, most of the research focuses on the performance, stability, robustness and efficiency of physical systems rather than security, which is broadly ignored, usually as a result of constrained factors, such as low processing, communication and adequate storage ability capacities. However, if security is disregarded, CPS will not work in a stable manner (Lu et al., 2014). In response to the real need to apply security methods to protect these interconnections, a tight coupling in the interconnections between physical and cyber controlling components is required. Security issues are not new; however, advances in technology make it necessary to produce new approaches to protect data from hazards (Nourian and Madnick, 2014). Additionally, CPS privacy is another serious issue that should be taken into consideration (Lu et al., 2014) in any proposed security solution.

1.1. *Contributions*

Several papers in the literature discuss CPS security and focus only on particular issues. For example, the focus in Neuman (2009) is on the physical control of the CPS, and the author offers some suggestions for protecting communication channels, real-time requirements and applications. In Lu et al. (2014), a security framework for CPS is proposed with a comprehensive analy-