Cyber-Physical System (CPS) Security Treats: Challenges and Solutions

Sayeed Sajal[1], Israt Jahan[1, 2] and Kendall Nygard[3]

[1]Department of Math & Computer Science, Minot State University
500 University Ave W, Minot, ND, 58707, sayeed.sajal@ndus.edu

[2]Department of Computer Science, Nueta Hidatsa Sahnish College
220 8th Ave E New Town, ND 58763, ijahan@nhsc.edu

[3]Department of Computer Science, North Dakota State University
1340 Administration Ave, Fargo, ND 58105, kendall.nygard@ndsu.edu

Abstract

Cyber-physical system (CPS) is a combination of cyber (computation and communication) and physical components which are interconnected with feedback loops. With the advancement of new technologies, the interconnectivity and complexity of the networks are increasing exponentially. Smart innovations such as the internet of things (IoT), smart cars, smart buildings added more functionality, flexibility, and convenience to our lifestyle. On the other hand, we are trapped into security threats and challenges. There are many areas that might face security vulnerability due to the rapid expansion of connectivity without considering proper security solution. In this work, we demonstrated the vulnerability in the systems due to security threats in CPS and their probable solutions are proposed.

1. Introduction

With the advancement of modern technologies and innovations [1-5], we are blessed with flexibility, convenience, and freedom. It makes our lives easier and convenient. For example, we don't have to go shopping mall to shop [6], we don't have to go to ticket counters to buy tickets [7], we can do online reservation without going to a restaurant [8]. We don't have to drive our self-driving [9] car while traveling, we don't have to be at a business location [10] to do business, we don't have to be at the location to monitor any power plant [11] and so on. We can't do any of those without a connected network. It is like a blessing to us if we can use our technologies by authorized personnel. On the other hand, it will be a nightmare if these services are driven by unauthorized personnel. Not only we lost all of our flexibility and convenience, but also, we are trapped by unlimited uncertainty. Without proper security, our services can be hacked by bad people and our life will be in their hand. More specifically, in the cyber-physical system [12-16], our physical components like cars, business location, power plants, medical equipment can be controlled by people who are not authorized to use those. That's one of the biggest challenges we encounter with the advancement of technologies in the connected world. We need to identify the top security threats in cyber-physical systems and the solutions to avoid those. With proper security measures [17-22], we can enjoy the innovative technologies with any concerns. That's the world, we all want to live happily and peacefully.

2. Flowchart of the CPS Functionality

In general, most of the CPS are structured for 4 main functions [23]. All of the 4 functions are shown in Figure 1.

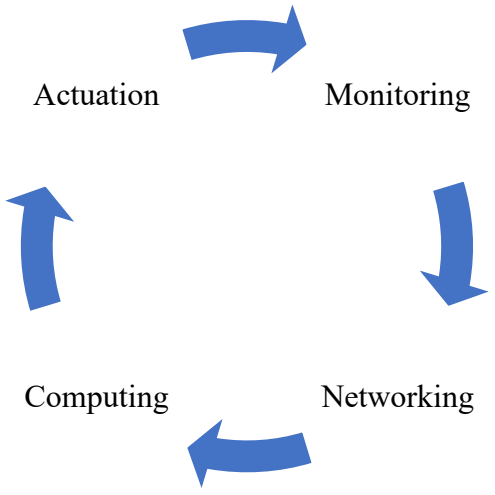

Figure 1: Flowchart of the CPS functionality

A. Monitoring

To monitor the environment and physical process of any system is a fundamental function of CPS. It is necessary to be vigilant to make sure the system is operating as expected.

B. Networking

There are a lot of sensors connected to a CPS and it's very important and crucial to connect all the sensors in a network to function properly. This phase deals with data acquisition, aggregation and diffusion. All the sensors generate data in real-time, various sensors could generate much data which is to be aggregated or diffused for analyzers to process further. In addition, different applications need to interact with networking communication.

C. Computing

In this phase, all the collected data from the sensors during the monitoring phase are analyzed with intelligence to check whether the physical process satisfies certain pre-defined criteria. If the criteria are not being satisfied, the corrective actions are proposed to be executed in order to fix the issue.

D. Actuation

This phase executes the actions determined during the computing phase. Actuation can actuate various forms of actions such as correcting the cyber behavior of the CPS, changing the physical process and execution physical activities.

3. Major Cyber-Physical System Security Threats

A. Eavesdropping

Eavesdropping refers to the attack that adversary can intercept any information communicated by the system [24]. It is a passive attack where the attacker does not interfere with the working of the system and simply observes its operation. CPS is particularly susceptible to eavesdropping through analysis such as intercepting the monitoring data transferred in sensor networks collected through monitoring phase. It violates user's privacy such as a patient's personal health status data transferred through the system.

B. Compromised-Key Attack

A key is a secret code which is necessary to interpret secure information. Once an attacker obtains a key, then the key is considered a compromised key [25]. It is used to gain access to a secured communication without the perception of sender or receiver. The attacker can

decrypt by the compromising key, then try to use the compromised key to compute additional keys, which could allow the attacker access to other secured communications or resources. Having control of the secured communication system, the attacker can manipulate and sensors and actuators.

C. Man-in-the-Middle Attack

In man-in-the-middle attack [26], false messages are sent to the operator and can take the form of a false positive or a false negative. This may cause the operator to take an action, such as flipping a breaker when it is not required, or it may cause the operator to think everything is fine and not take an action when an action is required.

D. Denial-of-Service Attack

Denial of Service (DoS) attack [27] is one of the network attacks that prevent legitimate traffics or requests for network resources from being processed or responded by the system. This attack usually transmits a huge amount of data to the network to make busy handling the data so that normal services cannot be provided. The denial-of-service attack prevents normal work or use of the system. After gaining access to the network of cyber-physical systems, the attacker can always do harm breaching the security of the cyber-physical system.

4. Types of Attacks:

According to the ISO/IEC 27001:2013 standard, threats may be deliberate, accidental or environmental. The examples of typical threats include physical damage, natural events, loss of essential services, radiation malfunctions, compromise of information (for example, eavesdropping, tampering with software, etc.), technical failures, unauthorized actions (for example, data corruption), compromise of functions (for example, forging and abuse of rights). Based on the results of the analysis of existing studies in security in Figure. 2, a "tree" of attacks and threats based on the functional model of CPS [28] is proposed. Branches of the "tree" include the following types of attack:

a) attacks on sensor devices (Sensing)

b) attacks on actuators (Actuation)

c) attacks on computing components (Computing)

d) attacks on communications (Communication)

e) attacks on feedback (Feedback)

Figure 2: A tree diagram of attacks and threats on cyber-physical systems.

5. Security Solutions

A. SCADA Systems Security

Supervisory Control and Data Acquisition (SCADA) systems are responsible for data acquisition and supervisory control [29]. A model that simulates attempts by a highly skilled attacker to execute a premeditated malevolent scheme and calculates the probability of the attacker's mission success was proposed in [30].

B. Smart Grid Security

In [31] a novel cyber-physic fusion approach by developing an abnormal traffic-indexed state estimation (ATSE) method for attack detection in Smart Grid was described. ATSE was applied to detect the attacks, including IDS (Snort) and bad data detection algorithm (Chi-square Test). The basic idea of ATSE is that the discrete event is quantified as the index of a physical system model. It demonstrates a low-cost and easy-implement solution to integrate heterogeneous data in Smart Grids. ATSE could be extended to detect other attacks in various CPS.

C. Communication Security

Genge et al. [32] have described the problem of how network parameters, such as packet loss, communication delay, timing management logic, and network traffic can affect the consequences of attacks. The main contribution of the authors is that the most important parameters that could affect the stability of physical processes were identified. The authors noted that communication parameters (for example, communication delay) have a limited impact on the result of the attacks and the scheduling parameters of the tasks can affect the stability of physical processes.

D. Control Security

It can be divided into actuation security and feedback security. Actuation security aims to ensure that actuation can take place under the appropriate authorization. Dynamic specification of the authorizations will be designed as CPS's requirements change over time. Feedback security refers to ensuring that the control systems in a CPS which provide the necessary feedback for effecting actuation are protected. The state-of-art security solutions mainly focus on data security only, but their effects on estimation and control algorithms have to be studied for providing in-depth defense against various attacks on CPS.

E. Sensing Security

The security configuration, if depending on the context; we have to ensure that context information is trustworthy. Here we propose that in the lifecycle of the security-relevant context from context discovery, context acquisition to context convey, we adopt Trusted Platform Module to achieve the goal of secure sensing

F. Countermeasures Against Cyber-attacks

Due to the increasing use of IoT and Internet of Autonomous Vehicles in the near future VANETs (Vehicular ad hoc networks) develop continuously and attract increased attention. An attacker could compromise some vehicles and turn them into zombie vehicles, awaiting orders from a command and control server. In [33] the approaches for intrusion/misbehavior detection were provided. Proactive and reactive solutions that could be employed as countermeasures to attacks were also discussed.

6. Conclusion

Here, we discussed the major cyber-physical security threats and probable security measure. To protect a CPS from any security threats, we need to make sure we considered all possible threats and security vulnerabilities. With the advancement of new technology like the Internet of Things (IoT), new threats might make our CPS more vulnerable. Having

the right security measures and continuous research to defend new threats can protect the CPS from evil hands. We hope that this survey will motivate further research to protect humanity from evils.

References

1. Chinnery, G. M. (2006). Emerging technologies: Going to the MALL: Mobile-assisted language learning. *Language learning & technology*, *10*(1), 9-16.

2. Alexander, A. D. (1972). Impacts of telemation on modern society. In *On Theory and Practice of Robots and Manipulators* (pp. 121-136). Springer, Berlin, Heidelberg.

3. Slovic, P. (2013). *Risk, media and stigma: Understanding public challenges to modern science and technology*. Routledge.

4. Edmundson, A. (Ed.). (2006). *Globalized e-learning cultural challenges*. IGI Global.

5. Garson, G. D. (Ed.). (2007). *Modern Public Information Technology Systems: Issues and Challenges: Issues and Challenges*. Igi Global.

6. Forsythe, S., Liu, C., Shannon, D., & Gardner, L. C. (2006). Development of a scale to measure the perceived benefits and risks of online shopping. *Journal of interactive marketing*, *20*(2), 55-75.

7. Law, R., & Leung, R. (2000). A study of airlines' online reservation services on the Internet. *Journal of Travel Research*, *39*(2), 202-211.

8. Kaakinen, H., & Purkayastha, E. (2016). ONLINE MARKETING OF HOSPITALITY SERVICES: Tourist satisfaction with online accommodation booking.

9. Levinson, J., Askeland, J., Becker, J., Dolson, J., Held, D., Kammel, S., ... & Sokolsky, M. (2011, June). Towards fully autonomous driving: Systems and algorithms. In *2011 IEEE Intelligent Vehicles Symposium (IV)* (pp. 163-168). IEEE.

10. Schafer, J. B., Konstan, J. A., & Riedl, J. (2001). E-commerce recommendation applications. *Data mining and knowledge discovery*, *5*(1-2), 115-153.

11. Boost, M., & Bizouard, J. (2003). *U.S. Patent No. 6,532,425*. Washington, DC: U.S. Patent and Trademark Office.

12. Lee, E. A. (2008, May). Cyber-physical systems: Design challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)* (pp. 363-369). IEEE.

13. Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, *3*, 18-23.

14. Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In *Design Automation Conference* (pp. 731-736). IEEE.

15. Derler, P., Lee, E. A., & Vincentelli, A. S. (2012). Modeling cyber-physical systems. *Proceedings of the IEEE*, *100*(1), 13-28.

16. Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The impact of control technology*, *12*(1), 161-166.

17. Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K., & Chow, K. P. (2010, December). Security issues and challenges for the cyber-physical system. In *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing* (pp. 733-738). IEEE.

18. Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In *2011 International conference on the internet of things and 4th international conference on cyber, physical and social computing* (pp. 380-388). IEEE.

19. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831.

20. Ashok, A., Hahn, A., & Govindarasu, M. (2014). Cyber-physical security of wide-area monitoring, protection, and control in a smart grid environment. *Journal of advanced research*, *5*(4), 481-489.

21. ZHANG, L., Qing, W. A. N. G., & Bin, T. I. A. N. (2013). Security threats and measures for the cyber-physical systems. *The Journal of China Universities of Posts and Telecommunications*, *20*, 25-29.

22. Morris, T. H., Srivastava, A. K., Reaves, B., Pavurapu, K., Abdelwahed, S., Vaughn, R., ... & Dandass, Y. (2009, October). Engineering future cyber-physical energy systems: Challenges, research needs, and roadmap. In *41st North American power symposium* (pp. 1-6). IEEE.

23. Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K., & Chow, K. P. (2010, December). Security issues and challenges for cyber-physical system. In 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing (pp. 733-738). IEEE.

24. Jung-Chun Kao and Radu Marculescu, "Eavesdropping Minimization via Transmission Power Control in Ad-Hoc Wireless Networks", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006.

25. K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis, and G. Stephanides, "Two Types of Key-Compromise Impersonation Attacks against One-Pass Key Establishment Protocols", Communications in Computer and Information Science, Volume 23, Part 3, 227-238, 2009.

26. Roi Saltzman, Adi Sharabani, "Active Man in the Middle Attacks, A Security Advisory", A whitepaper from IBM Rational Application Security Group, February 27, 2009.

27. Pelechrinis K., Iliofotou M., "Denial of Service Attacks in Wireless Networks: The case of Jammers", UC Riverside Department of Computer Science and Engineering, 2006

28. A. Hahn, R.K. Thomas, I. Lozano, A. Cardenas, A multi-layered and kill-chain based
security analysis framework for cyber-physical systems, Int. J. Crit. Infr. Prot. 11 (2015) 39–50.

29. Cai, N., Wang, J., & Yu, X. (2008, July). SCADA system security: Complexity, history and new developments. In *2008 6th IEEE International Conference on Industrial Informatics*(pp. 569-574). IEEE.

30. Y.F. Khalil, A novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures, Process Saf. Environ. Prot. 102 (2016)473–484.

31. T. Liu, Y. Sun, Y. Liu, Y. Gui, Y. Zhao, D. Wang, C. Shen, Abnormal traffic-indexed
state estimation: a cyber-physical fusion approach for Smart Grid attack detection, Future Gen. Comput. Syst. 49 (2015) 94–103.

32. B. Genge, C. Siaterlis, M. Hohenadel, Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems, Int. J. Comput. Commun. Control 7 (2014) 674–687.

33. F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: vANETs and IoV, Ad Hoc Networks 61 (2017) 33–50.