Security Issues of Cyber Physical System: A Review

Piyush Maheshwari
Lecturer
Department of Computer Applications
Institute of Engineering & Technology
Mangalayatan University Aligarh

ABSTRACT
Cyber Physical System (CPS) is extensively used in various fields like critical infrastructure control, vehicular system and transportation, social networking, medical and healthcare systems. The security concern for CPS is of utmost importance. CPS is vulnerable to many kinds of attacks that may cause major loss and potential security risk. In this paper, we will elaborate the requirement of security in CPS on the basis of attacks on CPS taking into account the existing security issues and the challenges to provide the security.

Keywords
Cyber Physical System (CPS), security, attack.

1. INTRODUCTION
CPS is a new type of system that integrates computation with physical processes. Components of cyber physical system (e.g., controllers, sensors, actuators, etc.) transmit the information to cyber space through sensing a real world environment; also they reflect policy of cyber space back to the real world [1].

CPS is physical and engineered system whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. This intimate coupling between the cyber and physical will be manifested from the Nano-world to large-scale wide-area systems of systems. The internet transformed how humans interact and communicate with one another, revolutionized how and where information is accessed, and even changed how people buy and sell products. Similarly, CPS will transform how humans interact with and control the physical world around us. [2]

Cyber physical systems may consist of many interconnected parts that must instantaneously exchange, parse and act upon heterogeneous data in a coordinated way. This creates two major challenges when designing cyber physical systems: the amount of data available from various data sources that should be processed at any given time and the choice of process controls in response to the information obtained. An optimal balance needs to be attained between data availability and its quality in order to effectively control the underlying physical processes. [3]

1.1 A CPS has characteristics like distributed management and control, high degree of automation**,** real time performance requirements, reorganizing/reconfiguring dynamics, multi-scale and system of systems control characteristics, networking at multiple scales**,** wide distribution geographically with components in location that lack physical security, integration at multiple temporal and spatial scales and take input and possible feedback from the physical environment. CPS objective is to monitor the behaviour of physical processes and actuating actions to change its behaviour in order to make the physical environment work correctly and in better way.

1.2 There are four main steps in CPS workflow as described by Eric Ke Wang, in Security issue and challenges in CPS (2010), Monitoring, Networking, Computation and Actuation.

1.2.1 Monitoring refers to give feedback on any past actions which are taken by the CPS and ensure correct operations in future. Monitoring of physical processes and environment is the basic function of CPS.

1.2.2 In networking phase, if there is much more than one sensor in CPS, all sensors can generate data in real time and many of them could generate much data which is to be aggregated or diffused for further processing for analyzers. At the mean time different applications need to be interacted with communication by networking.

1.2.3 Computing phase refers to reasoning and analyzing the data collected during monitoring for cross-checking that the physical processes are satisfying prescribed criteria or not. If not so then corrective actions which have been proposed before can be executed in order of ensuring the meeting criteria.

1.2.4 Actuation phase is used to execute the actions find in the computing phase. It can correct the cyber behavior of CPS and can change physical process and many other forms of actions as per the need.

Few example based on above given characteristics included by Siddhartha Kumar Khaitan, James D. McCalley, [4] that in modern power grid CPS , wind farm and solar farm constitute the physical resources, and data are collected from the sensors of these resources, which constitute the cyber part of the system. Often, a communication channel is involved to transmit data that are used to monitor and control the physical resources. On the cyber side, computations are carried out with the objective of maximizing utilization of renewable sources, and a suitable decision is taken, based on which the physical resources are further controlled. Another example is the body sensor network, which is a network of medical devices that can sense, actuate, and communicate with each other through a wireless network. An aircraft can be also seen as a CPS whose smart sensors and networking system enable it to monitor its operation while coordinating with ground stations.

A cyber-physical system (CPS) is a composition of independently interacting components, including computational elements, communications and control systems. Applications of CPS institute at different levels of integration, ranging from mobile CPS, data centers, networking systems, social networking and gaming, surveillance, electric power grid and energy systems, power and thermal management, nation-wide power grids, to medium scale, such as the smart home and buildings, and small scale, e.g. ubiquitous health care systems including implantable medical devices. Cyber-physical systems

primarily transmute how we interact with the physical world, with each system requiring different levels of security based on the sensitivity of the control system and the information it carries. Considering the remarkable progress in CPS technologies during recent years, advancement in security and trust measures is much needed to counter the security violations and privacy leakage of integration elements. [5]

1.3 Security is must in CPS , It is necessary for assuring that the systems are trustworthy, secure, and protect the privacy of information. For example, Patients depending on implanted medical devices want protection of their identity and critical health information that could be exposed via the connection of their devices to monitoring networks. Industry requires protection of intellectual property as well as sensitive business and demographic information. Assuring the confidentiality of information and controlling the access and use of data are challenging, especially as the systems that collect, manage, and analyze information are rapidly evolving and in some cases need to operate in a distributed or relatively open environment.

The paper is structured in 6 different sections such as *section1* presents the basic concept of CPS characteristics, workflow, need of security in CPS and fundamental definitions of CPS, *section 2* presents the literature review of various attacks, *section 3* discusses the CPS security objectives, *section 4* highlights the various types of attacks, its working method and impact on CPS, *section 5* represents the security methods and challenges against various types of attacks and *section 6* covers the conclusion part of the paper.

2. LITERATURE REVIEW ON VARIOUS ATTACKS

A. E. Gamal et al.. in 2005 proposed a model to allow arbitrary user distributions and study their impact on the eavesdropping risk, Jung-Chunn et al. in 2006, addressed about cryptographic techniques, secure routing and anonymous routing for preventing eavesdropping attack and also addresses important issues in designing such cryptosystems as key management, authentication and encryption/decryption algorithms [13].A. Aysu et al in 2013 addressed field programmable gate arrays (FPGAs) lattice-based cryptography technique to provide low-resource yet high performance FPGA device security to change the configuration of the control network to respond to cyber-attacks.

Diffie-Hellman et al.. in 1976 addressed about introduction of key exchange, in which there has been a large number of key establishment protocols proposed, including recent one-round by Jeong, I., Katz et al. and Law, L., Menezes et al. in 2004 and 1998 respectively, two-round by Bird, R. Gopal et al. and Lu, R., Cao et al.. in 1992 and 2005 respectively and three-round approaches by Blake-Wilson at al,Boyd et al. and Kwon et al. in 1999, 2004 and 2001 respectively. K. Chalkies et al. in 2009 addressed about two basic categories of protocols, the first includes so-called key transport protocols, in which the session key is created by one entity and is securely transmitted to the other. A second category includes key agreement protocols, where information from both entities is used to derive the shared key for preventing Compromised-Key Attack [14].

Agah et al.. in 2004 formulated a cooperative game between sensor nodes in mobile wireless sensor networks and showed that through cooperation between two nodes the data communication between them will be more reliable, S. Roy et al. in 2010 investigated the existing results about enhancing network security under the game-theoretic framework and provided a classification of recent results based on the types of the corresponding games, Y. Mo and B. Sinopoli in 2012 addressed a CPS model as a discrete linear time-invariant system against integrity attack where they presented a quantitative index of the system resilience by investigating the feasible set of the the adversary's attack strategies without being detected and the corresponding state estimation error under certain attacks, Yuzhe et al. in 2013 proposed a game-theoretic approach which provides an alternative way to handle two sided of the CPSs security interactive decision issues (defender and attacker)for Jamming attack [15]

Yuan et al. in 2013 addressed optimal attack scheduling schemes and intruder detection mechanism for the expected average estimation error and the expected terminal estimation error for preventing Denial-of Service attack. [16], Y. Yuan et al. in 2013 designed resilient controllers for cyber-physical control systems

under DoS attacks which they establish a coupled design framework which incorporates the cyber configuration policy of Intrusion Detection Systems (IDSs)and the robust control of dynamical system and also proposed design algorithms based on value iteration methods and linear matrix inequalities for computing the optimal cyber security policy and control laws for preventing Denial-of Service attack [21].

P. Shuanghe and H. Zhen and K.-J. Lin et al. in 2009 and 2012 addressed Trusted Platform Module (TPM) which is often added as a means to secure cryptographic key functionality, endorsement services, critical data storage, and integrity measurements, K. Xiao and M. Tehranipoor in 2013 addressed the built-in self-authentication (BISA) technique uses digitally signed filler cells to prevent and detect Trojans from occupying unused spaces in critical components, Y. Gilad et al. in 2014 addressed another approach ARM's Trust Zone architecture, which partitions applications into either the normal world (NWorld) or the secure world (SWorld) resource groups based on their level of trust for preventing Man-in-the-Middle Attack [18].

S. Amin et al. in 2010 addressed a resilient control problem where the control packets sent over a communication network are corrupted by human adversaries, K. Cheolhyeon et al. in 2013 addressed a general deception attack model and also described necessary and sufficient conditions that allow the attackers to perform the deception attacks without being detected by the monitoring system using the steady-state KF(Kalman filter),an Unmanned Aerial Vehicle (UAV) navigation example was also considered for more elaborating the deception attack.[19],G. Sabaliauskaite and A. Mathur in 2014 addressed another approach Intelligent Checkers which help to protect against stealthy deception attacks by raising an audible and visual alarm to alert system operators if a system anomaly is detected. [20]

3. CPS SECURITY OBJECTIVES

To assure the security of cyber physical system, there are following security objectives to achieve. Fig.1 depicts the various security objectives of CPS.

Figure 1:- Security objectives ofCyber Physical System

3.1 Confidentiality

Confidentiality refers that CPS should have the ability to safe the disclosure to unauthorized individuals or systems. For example, in a healthcare CPS, personal health record of any patient can be transmit from local repository or devices to the clinician or analyzer center. The healthcare CPS should maintain confidentiality by securing the transmitted data, restricting the places storing patients' personal health record, limiting access to these storing places. Disclosure of health data in any way results in a doubt of the system's confidentiality. If unauthorized person access these record, a notification of confidentiality leak should be occurred. It ensures that all sensitive information generated within the system is disclosed only to those who are supposed to see it

3.2 Integrity

Integration means modification in any resource or data can be possible after authorization. To ensure integrity of data, CPS requires the capability to detect any changes introduced by unauthorized activity or maliciously in the massage being passed. It ensures that all information generated and exchanged during the system's operation is accurate and complete without any alterations.

3.3 Availability

Availability in CPS refers to provide service every time by preventing computing, controls, and communication corruptions due to failures in hardware, system up gradation, power outages reason or by any attacks. It ensures that any entity which uses the data and services and resources of the system are able to do when required.

3.4 Reliability

Reliability in CPS refers to ensure that the data, transactions, communications are genuine. In CPS, the reliability aims to realize originality check in all the related process such as monitoring, networking, computing and actuation.

3.5 Robustness

Robustness of CPS implies a system quality which describes the degree to which a system is capable to work properly and effectively even in the presence of wrong inputs, malfunctions, disturbance. [8]

3.6 Trustworthy

Trustworthiness in CPS implies extent to which the system can be relied upon to perform up to the mark and correctly the system tasks under predefined operational and environment conditions over a predefined time.

A threat is a violation of security [9]. A system needs to be guarded against them, in order to ensure its correct operation at all times. The execution of the threats is called an attack while the entities which execute these threats are called attackers. [10]

4. TYPES OF ATTACK IN CPS

Figure 2:- Types of attacks in Cyber Physical System

As shown in fig.2 attacks in CPS can be categorized in six categories based on its impacts on the system.

Types of attacks: In literature various types of attacks has been discussed by the different authors [6,7]. The different types of attacks are summarized as follows:

Eavesdropping: It is a passive attack. Eavesdropping in CPS refers that attacker, rather than involving himself directly with the functioning of CPS; he just observes its operations and latterly uses this information to violate users' privacy such as patients' personal health data in a medical cyber physical system. With the help of such attacks the attacker adversary can intercept any information communicated by the system through monitoring or by traffic analysis.

Denial-of-Service Attack: In such type of attack the attacker floods the entire sensor network or controller with traffic until a shutdown occurs due to the overload. It sends invalid data to system networks, which causes abnormal termination of processes. It also blocks traffic, which results in a loss of access to network resources by genuine elements in 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.

Stealthy Deception Attack: This is an active attack in which attacker tamper with system components or data and don't

concern whether they can be detected by detection system or not. Deception attack is defined when the integrity of the sensor and control data packets has been breached.

Jamming Attack: In such attacks the attacker may jam the wireless channel between sensor nodes and the remote estimator in a CPS.

Compromised-Key Attack: In such type of key attack the attacker can gain the access to a secured communication, decrypt or modify data and try to use the compromised key to compute additional compromised keys, which could allow the attacker access to other secured communications or resources. It is possible for an attacker to obtain a key although the process maybe a difficult and resource intensive. For example, the attacker could capture the sensors to execute reverse engineering job in order to figure out the keys inside.

Man-in-the-Middle Attack: In such type of key attack the attacker can gain the access to a secured communication, decrypt or modify data and try to use the compromised key to compute additional compromised keys, which could allow the attacker access to other secured communications or resources. It is possible for an attacker to obtain a key although the process maybe a difficult and resource intensive. For example, the attacker could capture the sensors to execute reverse engineering job in order to figure out the keys inside.

5. SECURITY METHODS OF CPS AGAINST VARIOUS TYPES OF ATTACKS

Table 1 shows, the various security methods for preventing attacks of CPS.

S.N.	Types of Attack	Technology	Security Methods	Ref. No.
1	Eavesdropping	Confidentiality security property ensures that it can be avoided.	Cryptosystem (symmetric, Asymmetric), secure routing and anonymous routing.	[13]
2	Denial-of-Service Attack	The availability security property ensures that it can be avoided.	Discretionary Access Control (DA), Mandatory Access Control (MA), Access Control Lists (ACLs), Role based Access Control (RBAC).	[21]
3	Stealthy Deception Attack	The Integrity security property ensures that it can be avoided.	Resilient control system methodology	[11,19,20]
4	Jamming Attack	The Integrity security property ensures that it can be avoided.	Discrete linear time-invariant system model, Game-theoretical framework.	[15]
5	Compromised-Key Attack	Confidentiality security property ensures that it can be avoided.	Cryptography, key transport protocols and key agreement protocols, one round two round and three round approaches for key establishment protocol one-pass two-party key establishment Protocols.	[12,14]
6	Man-in-the-Middle Attack	Authentication, authorization along with confidentiality and integrity protection are needed to stave of this attack.	Message digest, digital signature, MAC, biometrics, Trusted Platform Module (TPM)	[17,18,22]

6. CONCLUSION

The innovation of CPS to change every aspect of life is unaccountable. This can be further emphasized from the fact that CPS has been the top priority concern by major international agencies and policy making organizations. These systems depend on a computational core that is tightly conjoined and coordinated with components in the physical world. As systems evolve they will rely on human decision making into new, more strategic aspects and will increasingly rely on operational human knowledge through computational intelligence. The attacks on CPS result into making the system dysfunctional. This leads to a chain of problems to individuals and organizations and various serious financial losses too. Many organizations have to pay heavy losses for such attacks. There is need of new architectures, model-based design methods and tools that provide security mechanisms for prevention, detection and recovery, resilience, and deterrence of attacks. This paper by various authors has addressed some such issues incorporating the range from objectives to the probable solutions of these attacks.

7. REFERENCES

[1]. Park, K. J., Zheng, R., and Liu, X., "Cyber-physical systems: Milestones and research challenges". Computer Communications. 36,1 , 2012, 1-7.

[2]. Ragunathan (Raj) Rajkumar, Insup Lee, LuiSha , John Stankovic "Cyber-Physical Systems: The Next Computing Revolution" , Anaheim, California, USA,Design Automation Conference,2010.

[3]. Andrei Petrovski, PrapaRattadilok, Sergei Petrovski, "Designing a Context-Aware Cyber Physical System for Detecting Security Threats in Motor Vehicles", ACM, 2015.

[4]. Siddhartha Kumar Khaitan, James D. McCalley, *"* Design Techniques and Applications of Cyber physical Systems: A Survey*"* IEEE SYSTEMS JOURNAL, 2014.

[5]. CharalambosKonstantinou!,MichailManiatakos!, FareenaSaqib†, Shiyan Hu‡, Jim Plusquellic§ and Yier Jin, "Cyber-Physical Systems: A Security Perspective", 20th IEEE European Test Symposium (ETS), 2015.

[6]. Tianbo Lu1,2, Jinyang Zhao1, Lingling Zhao1, Yang Li1 and Xiaoyan Zhang1, "Towards a Framework for Assuring Cyber Physical System Security", International

Journal of Security and Its Applications Vol. 9, No. 3 , 2015, pp. 25-40

[7]. Eric KeWang,Yunming Ye, XiaofeiXu, S.M.Yiu, L.C.K.Hui, K.P.Chow , "Security Issues and Challenges for Cyber Physical System", IEEE/ACM International Conference on Green Computing and Communications &2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing , 2010

[8]. Dr. Nabil Adam, "Workshop on Future Directions in Cyber-Physical Systems Security", Final Report January 2010.

[9]. M. Bishop. Computer Security: Art and Science. Addison-Wesley Professional, 1st edition, 2002.

[10]. Krishna Kumar Venkatasubramanian, "security solutions for cyber-physical systems",A Dissertation Presented in Partial Fulfillmentof the Requirements for the DegreeDoctor of Philosophy Arizona State University, December 2009.

[11]. Fabio Pasqualetti, "Attack Detection and Identification in Cyber-Physical Systems", IEEE transactions on automatic control, vol. 58, no. 11, november 2013.

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

[13]. J.-C. Kao and R. 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), pp. 707-714.

[14]. 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, vol. 23, (2009), pp. 227-238.

[15]. L. Yuzhe, S. Ling, C. Peng, C. Jiming and D. E. Quevedo, "Jamming attack on Cyber-Physical Systems: A game-theoretic approach," Cyber Technology in Automation, Control and Intelligent Systems (CYBER), 2013 IEEE 3rd Annual International Conference on, (2013), pp. 252-257.

[16]. Z. Heng, C. Peng, S. Ling and C. Jiming, "Optimal DoS attack policy against remote state estimation," Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on, (2013), pp. 5444-5449.

[17]. UttamAdhikari, "Event and intrusion detection systems for cyber-physical power systems" ,Doctoral Dissertations, Mississippi State, MississippiAugust2015.

[18]. Kevin G. Lyn, "Classification of and Resilience to Cyber-Attacks on Cyber-Physical Systems",Doctoral Dissertations, Georgia Institute of Technology, August 2015.

[19]. K. Cheolhyeon, L. Weiyi and H. Inseok, "Security analysis for Cyber-Physical Systems against stealthy deception attacks," American Control Conference (ACC), (2013), pp. 3344-3349.

[20]. AnisDrira, "Characterization of Optimal Cyber Attacks onControl Systems", Doctoral Dissertations, The University of Tennessee, Knoxville,December2015.

[21]. Y. Yuan, Z. Quanyan, S. Fuchun, W. Qinyi and T. Basar, "Resilient control of cyber-physical systems against Denial-of-Service attacks," Resilient Control Systems (ISRCS), 2013 6th International Symposium on, (2013), pp. 54-59.

[22]. R. Saltzman and A. Sharabani, "Active Man in the Middle Attacks, A Security Advisory", A whitepaper from IBM Rational Application Security Group, (2009) February 27.