A Study on Vulnerabilities and Collateral in Cyber Physical System

Pradosh Chandra Patnaik[a], M V Ramana Murthy[b], S B Kishor[c]
[a]Research Scholar in Dept. Of Computer Science, Gondwana University, Gadchiroli, Maharashtra, India
[b]Professor, Dept of Mathematics & Computer Science, Osmania University, Hyderabad, India
[c]Head, Dept. Of Computer Science, Sardar Patel Mahavidyalaya, Chandrapur, Maharashtra, India

---

Abstract

In this paper, we explore the security challenges and issues of cyber-physical systems. (1)We abstract the general workflow of cyber physical systems, (2)identify the potential vulnerabilities, attack problems and issues, characteristics and a collection of challenges that need to be addressed; (3)then we also suggest a context-aware security framework for general cyber-physical systems and advice some potential research areas and problems.

KEYWORDS- Cyber-Physical System, Security, actuation, context-aware

---

1. Introduction

Cyber-Physical System (CPS) [1] aims at examining and supervising the behaviour of physical processes, and actuating actions to transform its behaviour in order to make the physical environment work correctly and better. Commonly, a cyber physical system (CPS) consists of two major mechanisms, a physical process and a cyber system. Typically, the physical procedure is monitored or controlled by the cyber system, which is a associated system of several tiny devices with sensing, computing and communication capacity. The physical process involved may be a natural, a man-made physical system (e.g. a operation room) or a more complex combination of the two. However, as the communication between the physical and cyber systems improves or grows more, the physical systems become increasingly more liable to the security vulnerabilities in the cyber system. For example, some hackers have busted into the air traffic control mission-shore up systems of the U.S. Federal Aviation Administration many times in recent years, according to the report sent to the FAA in 2009 may [2]. Now few hackers are also able to hack those medical devices fixed in human body which have wireless interactions [3]. A CIA report[4] reveals that hackers have infiltrated power systems in several regions outside the United States, and in any case, one case caused a power outage affecting multiple cities. In 2010, the attacker verified a software tool called CarShark[5] which could slay a car engine remotely, turn off the brakes so the car would not stop and make application give wrong readings by observing communications between the electronic control units(ECUs) and insert wrong packets of data to take out attacks. In this year, hackers have planned a virus which can successfully attack Siemens plant-control system [6]. Actually, the safety vulnerabilities are being found in more and

more cyber-physical systems like smart transportation system, medical systems electronic power grid, and so on. Security of CPS has become a matter of concern of researchers. If we have a highly secured cyber physical systems then we have to consider the possible vulnerabilities on the systems.Actually, security for cyber physical systems is a comparatively a new area and not much work has been done in this regard. Like any other new areas, most of the attempts seems to be focused on mapping clarification from existing domains such as sensor networks which contribute to the networked operation and low capability features with CPS [7]. However, these answers were frequently not designed for CPS. As an example, consider an example of gas leaking in a smart building, the cyber-physical system of the gas department must assist with the one which monitors the wounded person's health to accomplish the set free mission. In usual situation, these applications are not dependent. But once there is urgency, all these applications need to communicate and share resources to fulfill the same goal. Conventional secure communication solutions are not developed for the interoperation among mixed applications. How to make sure that the system is still secure while interacting with another system is an issue of importance in cyber physical systems. There are also other new security issues for CPS that need to be addressed. In this paper, we first figure out and model the general flow of work of a CPS. Secondly, we identify the vulnerabilities, attacking models and challenger types; finally we suggest a new security framework for CPS and talk about a set of challenges and research troubles that need to be resoluted in the future.

II. GENERAL WORKFLOW OF CPS

A general workflow of CPS can be classified into four important steps:

1) Monitoring: Monitoring of physical processes and environment is a essential purpose of CPS. It is also used to give feedback on any past actions which are taken by the CPS and make sure correct operations in the future. The physical process is to achieve the original physical goal of the CPS.

2) Networking: It deals with the data aggregation, dispersion. There can be more than one sensor in CPS. These sensors can produce data in concurrent, various sensors could generate much data which is to be aggregated or diffused for analyzers to practice further. At the same time, different applications need to be communicated with networking communication.

3) Computing: It is for reasoning and analyzing the data composed during monitoring to verify whether the physical process assured certain pre-defined condition. If the conditions are not being fulfilled, the corrective actions are suggested to be executed in order to make sure meeting the conditions. For example, a datacenter CPS can have a replica to predict the temperature increase with respect to other scheduling algorithms, which can be used to find out future potential operations;

4) Actuation: Here, executions of the actions are determined during the computing phase. Actuation can actuate various forms of actions such as correcting the cyber

performance of the CPS, changing the physical procedure. For example, the action can be the release of some type of medicine in a medical CPS. Fig 1 shows a common workflow of CPS. Let Y represent the data acquisition from sensors, Z represent the physical data aggregation in-network, U represent the valid computed result of the physical system states which could advise controller to select valid commands, V represent the control commands sent to the actuators.

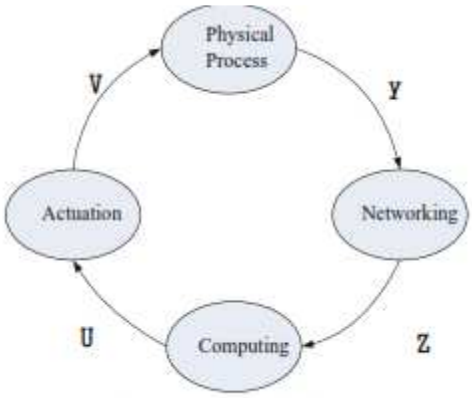

Figure 1. Abstraction of CPS

III. CPS SECRITY OBJECTIVES AND THREATS

A. Security Objectives

1) Confidentiality

Confidentiality refers to the capability to prevent the revelation of information to illegal individuals or systems [8]. For example, a Healthcare CPS on the Internet needs the individual health records to be transmitted from the Individual Health Record system to the doctor or front medical devices. The system efforts to enforce privacy by encrypting the individual health record during transmission, by limiting the places where it might appear (in databases, log files, backups, and so on), and by restricting access to the places where it is stored. If an illegal party obtains the individual health care in any way, a breach of privacy has taken place.. Confidentiality is essential for maintaining the users' isolation in Cyber Physical Systems [9]. Realizing Confidentiality in CPS must stop an enemy from intruding the state of the physical system by snooping on the communication channels between the sensors and the regulator, as well as between the regulator and the actuator.

2) Integrity

Integrity refers to data or resources cannot be modified without approval. Integrity is broken when an rival accidentally or with wontedly intends and modifies or deletes important data; and then the receivers get wrong data and believe it to be true. Integrity in CPS could be the ability to to get the physical goals by detecting , preventing, avoiding, or blocking deception attacks on the information sent and received by the sensors and the actuators or controllers [10].

3) Authenticity

In computing and communication procedure or process it is essential to make sure that the data, transactions, communications, transmission are genuine. It is also significant for authenticity to authenticate that both parties concerned are who they claim they are.[12] In CPS, the authenticity intends to realize authentication in all the related procedures like sensing, communications, actuations etc.

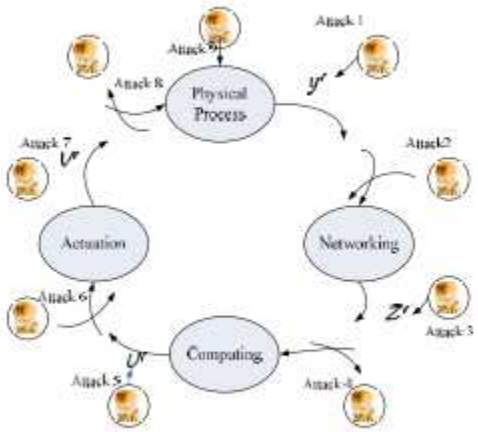

Figure 2. Attacks

B. Major types of attacks to CPS

As Figure 2 shows, we summarize the types of attacks to CPS as follows:

1) Compromised-Key

A key is a secret code/information which is important to read secure information. Once an attacker gets a key, then the key is considered a compromised key [14]. An attacker can gain access to secured information without the awareness of sender or receiver by using the compromised key. The attacker can decrypt or change data by the compromising key, and try to utilize the compromised key to compute additional keys, which could allow the attacker access to other secured communications or resources. Actually, it is possible for an attacker to obtain a key although the process maybe a difficult and resource concentrated. For example, the attacker could detain the sensors to execute reverse engineering job in order to figure out the keys inside, which could be represented in attack 9 shown in figure 3, or the attacker could pretend to be a valid sensor node to cheat to agree on keys with other sensors.

2) Eavesdropping

Eavesdropping refers to the attack that rival can intercept any information communicated by the system [13]. It is called passive attack that the attacker does not involve with the working of the system and simply finds its operation. CPS is particularly vulnerable to eavesdropping through traffic analysis such as intercepting the monitoring data

transmitted in sensor networks collected through monitoring. Eavesdropping also violates user's privacy such as a individual patients health status data transferred in the system. In Figure 2, attack 4 can represent the eavesdropping attacks on data aggregation processes; attack 8 can represent the tapping on controller demands.

3) Man-in-the-Middle Attack

In man-in-the-middle attack [15], wrong messages are sent to the operator, and can take the form of a wrong negative or a wrong positive. This may cause the machinist to take an action, such as flipping a breaker, when it is not needed, or it may cause the operator to think everything is fine and not take an action when an action is needed. For example, in Figure 3, attack 7 shows that the rival sends V' to indicate a system change, however, V' is not the real actuate command. When the operator follows normal procedures and attempts to correct the problem, the operator's action could cause an undesirable event. There are numerable variations of the modification and replay of control data which could impact the operations of the system. Attack 1, attack 3, attack 5 can also represent this kind of attacks.

4) Denial-of-Service Attack

Denial of Service (DoS) attack [16] is one of the network attacks that stop the legal traffics or requests for network resources from being responded or processed by the system. This type of attacks usually transmits a huge amount of data to the network to make demand handling the data so that normal services cannot be provided.

The denial-of-service assault prevents normal work or use of the system. After gaining access to the network of cyber physical systems, the attacker can always do any of the following:

--Flood a controller or the entire sensor network with traffic until a shutdown occurs due to the overload.

--Send invalid data to controller or system networks, which causes abnormal termination or behaviour of the services.

--Block traffic, which results in a loss of access to network resources by authorized elements in the system.

For instance, in Figure 2, Attack 2 can represent that adversaries flood the entire sensor network with a large amount of jamming data to block the normal network traffic, attack 6 can represent that the adversaries send a huge amount of invalid data to actuators to cause abnormal termination of actuation process.

C. Characteristics of Adversaries

This section introduces several main types of potential opponents:

(1) Skilled hackers are complicated programmers with the skill to find exclusive vulnerabilities in existing software and to create working make use of codes;

(2) Discontented insiders with malicious intent may not need a great deal of knowledge about cyber intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause injure to the system or to steal system data, who are considered a principal source of cyber crime and sabotage, the types of insiders may be employees, contractors, or business partners;

(3) Criminal groups, the main motivation of a criminal group launching an attack on a cyber-physical system would be extortion. [4]
(4) Nation-states terrorist group, most terrorists seek higher-crash targets in one country such as aero systems or 735 power grid system, they could develop the capabilities to bring down those critical cyber-physical facilities. Besides they almost certainly try to achieve the goal by recruiting highly skilled coders, hiring control system engineers and bribing insiders. [17]

Depending on the types of rivals, the defenders of CPS can adopt the corresponding policies or strategies to respond to the attack. Besides, researchers can gain understanding of rivals characteristics and an ability to anticipate an rival in order to build hazard models.

IV.CONTEXT-AWARE SECURITY FRAMEWORK

We propose a context-aware security framework for cyber physical system.

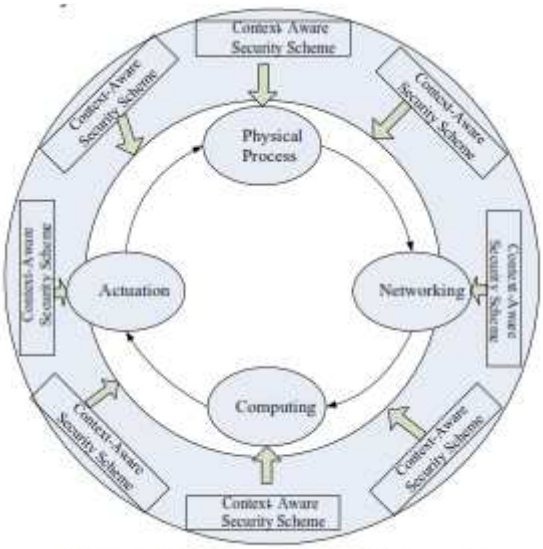

Figure 3. The context-aware security framework

As Figure 3 shows, we make security-relevant context information incorporated into several security measurements such as verification, encryption, key agreement protocol, access control and so on. Therefore, security mechanism for cyber-physical system can be vigorously adapting to the physical environment by the assistance of context coupling. We call this kind of security mechanism context-aware security framework.

Context is the set of environmental states and settings that either finds out an application's behavior or in which an application event happens [18]. The context can be from many context information providers and can be different forms from temperature to grade of pleasure. Commonly, the context can be categorized into four types: system context, user context, physical environment context and time context. In our framework, we mainly tackle security-relevant context which consists of the set of contextual attributes that can be used to characterize the situation of an entity, whose value affects the choice of the most appropriate controls or the configuration of those controls to

protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, reliability and availability. When attacks are happening, the attack model and the adversary types can also be one of the contextual attributes. The values of security-relevant contextual attributes affect the choice of the most appropriate controls because they impact the likelihood of certain threats to confidentiality, integrity, and availability being realized. Therefore, based on their values, the most suitable controls and configuration of those controls can be employed to alleviate those threats. The context-aware security framework can be represented as following formula; the general workflow can be referenced in Figure 4:

Let us consider one health care case, the operating doctor can be certified to access his patients' records when he is in hospital, while when the place sensing data shows he is outside, if the doctor still wants to access the records, the access control works joined with the changed context and deny this access.

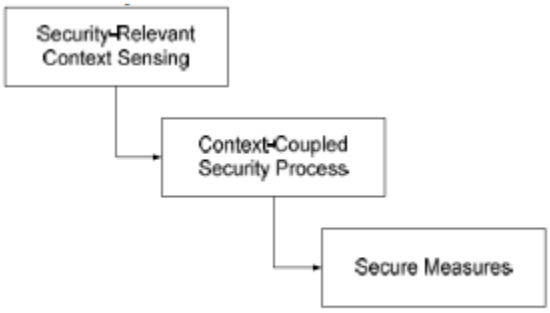

Figure 4. Workflow of general context-aware security scheme.

$$\{Security\ Processes\}_{context} \rightarrow Secure\ Measures$$

In the context-aware security framework for CPS, we separate it into 3 main aspects: sensing security, cyber security, control security, as show in Figure 5.

Sensing security: The security configuration, if depend 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. A Trusted Platform Module (TPM) [19] is a relatively cheap hardware component used to facilitate building trusted software systems. Our proposed solution leverages the TPM functionality of attesting to the integrity of software running on a sensor to a remote verifier. A TPM can be used to enable trusted boot, where each piece of code loaded from boot-time is measured via cryptographic hash [20] before loading. All important keys and data will be saved in the Basically the sensor node platform will consist of ARM11 chip, external memory Flash and SDRAM, Zigbee as transmitter, temperature sensor and battery operated power supply. Therefore, beside all the data is authenticated from the sensors to the verifiers with secret keys which are stored inside securely, potential loop holes are also blocked by embedding the memories, cryptographic eliminators and master key into the processor chip.

Cyber Security: It includes communication security and computing security. CPS is networked which not only allows them to form a network for data fusion, and delivery to back-end entities but also take coordinated response actions. We can design a context-incorporated communication protocols for securing both inter and intra CPS communication from both active (interferers) and passive (eavesdroppers) adversaries. It includes context aware key management scheme, context-aware mutual authentication scheme, and context-aware privacy protection scheme. Besides, once the data has been collected and processed it may be needd to be stored over time for future access; any tampering of the stored data can lead to errors or disruptions in future. In the future, context-aware encryption, digital signature, and access control solutions will be developed for securing data in CPS platforms against physical or cyber tampering and invalid access.

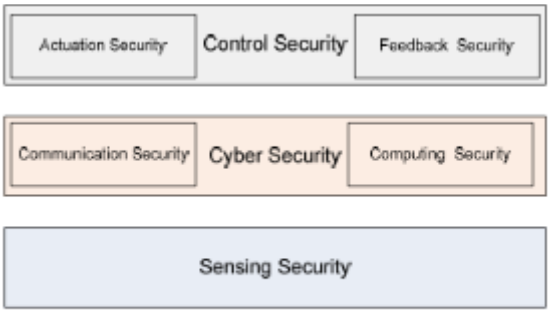

Figure 5. Main security aspects

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 condition of the authorizations will be designed as CPS's needs change over time. Feedback security refers to ensuring that the control systems in a CPS which provide the essential feedback for effecting actuation are protected. The state-of-art security solutions mainly focus on data security only, but their effects on decision and control algorithms have to be studied for providing in-depth defense against various attacks on CPS.

Context-aware privacy protection and encryption scheme mainly prevents the users' privacy from eavesdropping or data stealing. In the coming future, we will continue developing the rest of security protocols and schemas in the proposed context aware security framework for CPS. Context aware mutual authentication protocol resolves man-in-the middle-attacks and other authenticity problems; Context aware access control solves the unauthorized access problems; context-aware keys management scheme can process keys management for various CPS related applications and situations; Context-aware intrusion detection mainly detect invalid intrusion and block DoS attacks. And we will implement our security protocols and schemes for a prototype of CPS.

V. CONCLUSIONS

In this paper, we examine the security issues and challenges of Cyber-Physical Systems and suggest a security framework for CPS. We hope that these issues and challenges will

bring enough motivation for further discussions and interests of research work on security aspects for CPS.

REFERENCES

[1] Kaiyu Wan,K.L. Man,D. Hughes, "Specification, Analyzing Challenges and Approaches for Cyber-Physical Systems (CPS)", Engineering Letters,issue3, EL_18_3_14, 2010.
[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E.,
"Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002,pp. 393-422.
[3] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534
[4] Hollar, S, "COTS Dust", Master's Thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.
[5] Kelly O'Connell, "CIA Report: Cyber Extortionists Attacked Foreign Power Grid, Disrupting Delivery", Internet Business Law Services, http://www.ibls.com/internet_law_news_portal_view.aspx?id=1963& s=latestnews, 2008.
[6] J. A. Stankovic, I. Lee, A. Mok, and R. Rajkumar, "Opportunities and obligations for physical computing systems", IEEE Computer, 38(11):23–31, November 2005.
[7] Strulo, B., Farr, J., and Smith, A., "Securing Moile Ad hoc Networks — A Motivational Approach", BT Technology Journal, Volume 21, Issue 3, 2003, pp. 81 – 89.

[8] Jason Madden, Bruce McMillin, and Anik Sinha, "Environmental Obfuscation of a Cyber Physical System - Vehicle Example", Workshop on 34th Annual IEEE Computer Software and Applications Conference, 2010.
[9] Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and
Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.
[10] 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.
[11] Daniel Work, Alexandre Bayen and Quinn Jacobson, "Automotive Cyber Physical Systems in the Context of Human Mobility", National Workshop on High-Confidence Automotive Cyber-Physical Systems, Troy, MI, 2008.
[12] William Stallings, "Cryptography and network security: principles and practice", Prentice Hall, 5nd Edition, ISBN-10: 0-13-609704- 9,2010. 737
[13] 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.
[14] Feng Gui, "Development of a New Client-Server Architecture for Context Aware Mobile Computing", PHD Thesis, Florida International University, 2009.
[15] "Federal Plan for Cyber Security and Information Assurance Research and Development", Report by the interagency working group on cyber security and information assurance, April 2006.

[16] Pelechrinis K., Iliofotou M., "Denial of Service Attacks in Wireless Networks: The case of Jammers", UC Riverside Department of Computer Science and Engineering, 2006.
[17] Oniz, C. C, Tasci, S. E, Savas, E., Ercetin, O., and Levi, A, "SeFER: Secure, Flexible and Efficient Routing Protocol for Distributed Sensor Networks", from http://people.sabanciuniv.edu/~levi/SeFER_EWSN.pdf
[18] Roi Saltzman,Adi Sharabani, "Active Man in the Middle Attacks, A Security Advisory", A whitepaper from IBM Rational Application Security Group, February 27, 2009.
[19] Escrypt whitepaper, "Trusted Computing Technology for embedded Systems", 2009.
[20] Kulkarni, S. S., Gouda, M. G., and Arora, A., "Secret instantiation in adhoc networks," Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, May 2005, pp. 1–15.

[21] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Jounal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

.