Cyber Security - Security Problems and Encounters in Physical System

Miss.Tosal Bhalodia[1] Mr.Keyur Zala[2] Miss Debalina Nandy[3]
[1,3]Assistant Professor [2]CEO
[1,3]Department of Computer Engineering
[1,3]Atmiya Institute of Technology & Science, Rajkot, Gujarat [2]ILAXO Rajkot,Gujarat

Abstract— In this paper, we look into the security challenge and issue of cyber-physical systems which is placed physically somewhere as mentioned. 1. We summary the general workflow of cyber physical systems, 2. Identify the attack issues, possible vulnerabilities, adversary characteristics and a set of challenges that need to be address; 3. Then we also propose a physical-context-awareness of security framework for all-purpose cyber-physical systems in real time application and suggest some probable research areas and problems for security.

Key words: Cyber Security, authentication, context-awareness, Cyber & Physical System

I. INTRODUCTION

Cyber Security in Physical System (CSPS) [1] aims at monitoring the behavior of physical processes, and actuating actions to change its behavior in order to make the physical environment work correctly and better. Commonly, a Cyber Security in Physical System (CSPS) consists of two major components, a physical process and a cyber system. Typically, the physical process is monitor or restricted by the cyber system, which is a network system of several minute devices with sensing, computing and communication (often wireless) capabilities. The physical process caught up may be a natural phenomenon (e.g. a inactive volcano), a man-made bodily system (e.g. a surgical room) or a more complex mixture of the both.

As the contact between the physical and cyber systems increases, the physical systems become increasingly more vulnerable to the security vulnerabilities in the cyber system. For example, a few hackers have broken into the air traffic control systems of the U.S. Federal Aviation several times in current years, according to an Inspector General FAA in 2009 may [2]. At the present some hackers are also able to hack those medical devices implanted in human body, which have wireless communications [3]. A report[4] reveals that hackers have penetrated power systems in several regions outside the INDIA, and in at least one case caused a power outage affecting several cities. In 2010, the attackers demonstrated a software tool called CarShark[5] which could kill a car engine remotely, turn off the brakes so the car would not stop and make instruments false reading by monitoring communications between the electronic control units(Power Unit) and also insert fake packets of data to take out attacks. During this time, hackers have designed a virus which can successfully attack Siemens plant-control system [6].

The security vulnerabilities are found in more cyber-physical systems like electronic power grid, smart transportation system, and medical system, and so on. Researchers start to concern about the security of CSPS. When we have smarter and highly-confident cyber- physical systems, one should cautiously consider the possible vulnerabilities on these system. In fact, security for cyber- physical systems is a relatively new area and not more work has been done in this area. Like any other new fields, most of the effort seems to be focused on mapping solutions from existing domain such as sensor network which share the networked operation and low capability characteristics with CSPS [7]. However, these solutions were usually not designed for CSPS. from the time when an example, regard as an instance of gas leaking in a smart house, the cyber-physical system of the gas department must interact with the one which monitor the wounded person's health to accomplish the rescue work. In normal situation, these applications are independent, but once there is an emergency, all these applications need to act together and share resource to accomplish the same goal. Traditional secure communication solution are not designed for the inter-operation among diverse application. How to make sure that the system is still secure while interacting with another system is an important issue in cyber- physical system. There are also other new security issues for CSPS that needs to be concerned.

In this paper, we first abstract and model the general workflow of a CSPS. Secondly, we identify the vulnerabilities, attacking models and adversary types; finally we propose a new security framework for CSPS and discuss a set of challenges and research problems that need to be resolved in the future.

II. GENERAL WORKFLOW OF CSPS

A general workflow of CSPS can be categorized into four main steps:

1) Networking: This step deals with the data aggregation, diffusion. There can be much more than one sensor in CSPS. These sensors can produce data in real-time, a variety of sensors could produce to a large extent data which is to be aggregated or subtle for analyzers to process further. At the same time, different application need to be interacted with networking communication process.
2) Computing: This is for analysis and analyzing the data collected during monitor to check whether the physical process satisfy certain pre-defined criterion. If the criterion are not being fulfilled, the corrective action are proposed to be executed

in order to ensure meeting the criterion. For example, a data- center CSPS can have a model to predict the temperature rise with respect to various scheduling algorithms, which can be used to establish future operation.

3) Actuation: Step executes the action determined during the computing phase. Actuation can activate various forms of actions such as correcting the cyber behavior of the CSPS, changing the physical process. For example, the action can be the delivery of some type of medicine in a medical CSPS.
4) Monitoring: Monitoring of physical process and environment is a unique function of CSPS. It is also use to provide feedback on any past action which are taken by the CSPS and ensure correct operation in the future. The physical procedure is to achieve the original physical goal of the CSPS.

Fig 1 shows a general workflow of CSPS. Let y represent the data acquisition from sensors, z the physical data aggregation in-network, valid computed result of the physical system states which could advise controller to select valid commands, and control commands sent to the actuators.

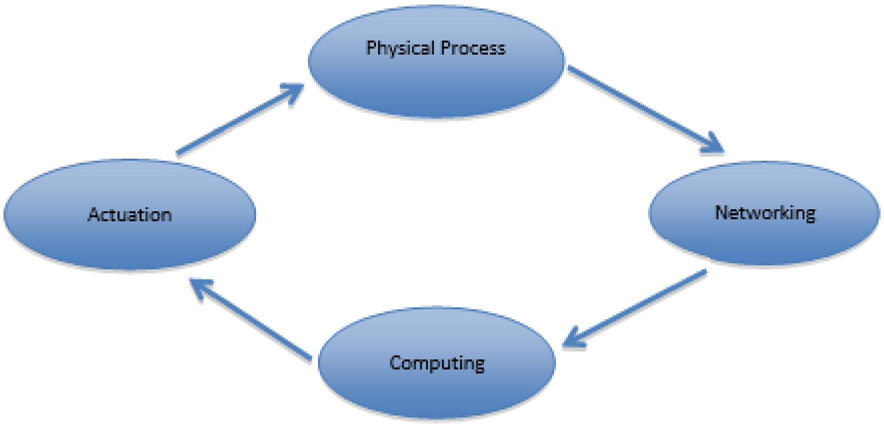

Fig. 1: Abstraction of CSPS

III. CSPS SECURITY OBJECTIVES AND THREATS

A. Security Objectives:

1) Confidentiality:

Confidentiality refer to the ability to stop the disclosure of information to unauthorized individuals or systems [8]. For example, healthcare CSPS on the Internet requires the individual health records to be transmitted from the individual Health Record system to the doctor or main medical device. The system attempt to enforce privacy by encrypting the personal health record during transmission, it is done by limiting the place where it might appear (in DB, log files, backup, and so on...), by restrict access to the places where it is saved. If an illegal party obtains the personal health care by any means, a breach of confidentiality will be occurred.

Confidentiality is essential (but not sufficient) for maintaining the user's privacy in Cyber Physical Systems [9]. Realizing Confidentiality in CSPS must prevent an challenger from infer the state of the physical system by eavesdrop on the communication channel between the sensor and the controller, as well as between the controller and actuator.

2) Integrity:

Integrity means related to data or resource, which cannot be modified without authorization. Integrity is disrupted when an opponent accidentally or with malicious engaged changes or delete important data or information; and then the receiver receive incorrect data and believe that the data is original one. Integrity in CSPS could be the capability to achieve the physical objectives by preventing, identifying, or blocking fraud attacks on the information sent and received by the sensors and the actuators or controllers [10].

3) Availability:

For any system to perform and achieve its purpose, the service must be present as when it is needed. That means the cyber system used to store and process the useful and important information, physical controls used to perform physical procedure, and the communication channel used to contact it must be functioning properly. High availability [11] of CSPS aims to always provide service by preventing calculations, control, and communication corruptions due to hardware failures or malfunctioning, system advancements, power cutoffs or denial-of-service attacks.

4) Authenticity:

For processing calculations and communication it is important to safeguard that the data, transaction, communication are authentic. It is also important for accuracy to validate that both the parties involved are authentic. [12] In CSPS, the authenticity purposes to realize authentication in all the connected process such as sensing, communications, and actuations.

B. Major types of attacks to CSPS:

Here summarize the types of attacks to CSPS as follows:

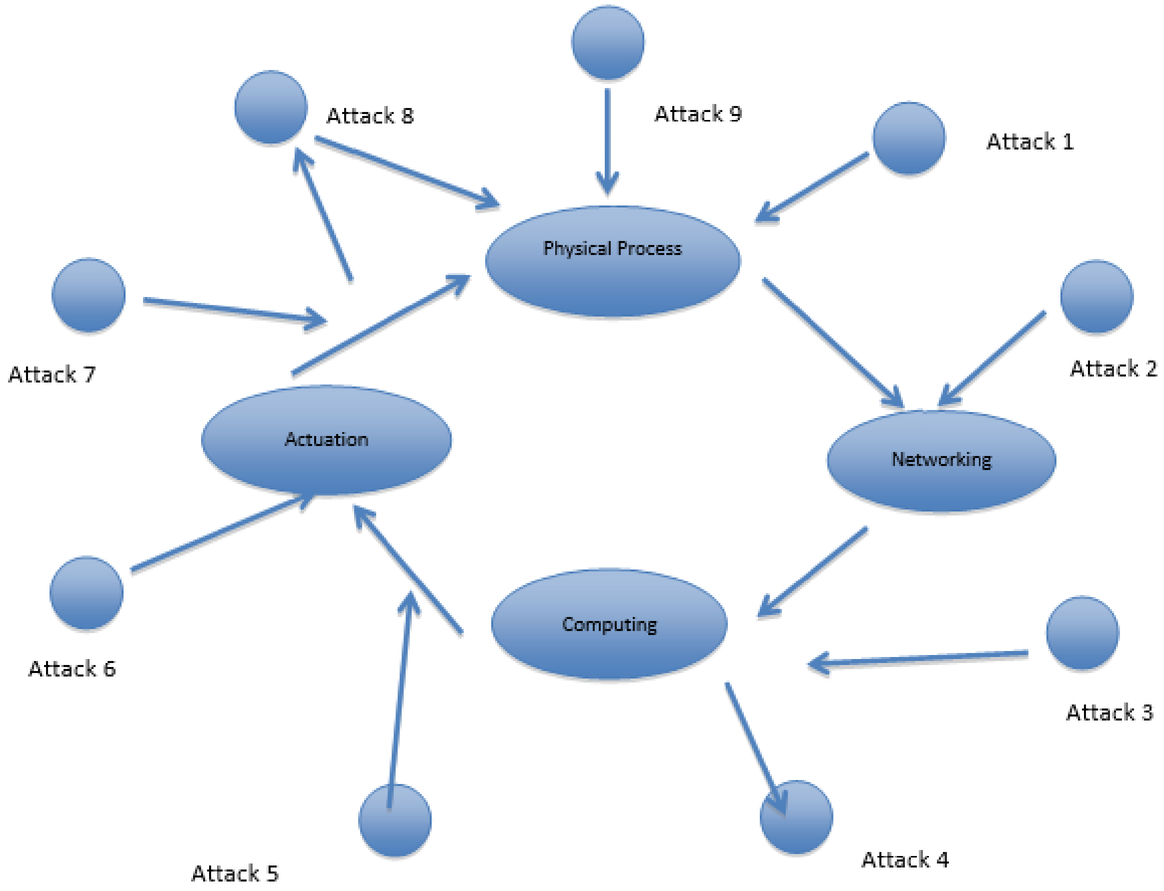

Fig. 2: Attacks

1) *Eavesdropping:*

Eavesdropping mentions to the attack that opposition can intercept any information or details communicated by the system [13]. It is also called passive attack that the enemy does not interfere with the working of the system and just observes its working operations. CSPS is particularly vulnerable to eavesdropping through traffic analysis such as interrupting the monitoring data transported in sensor networks collected through monitoring. Snooping also violates user's privacy such as a patient's personal details, health status data transported in the system. In Figure 2, attack 4 can denote the eavesdropping attacks on data accumulation processes; attack 8 can represent the tapping on controller loads.

2) *Compromised-Key Attack:*

A key is referred as a secret code, which is essential to interpret secure and important information. Once an invader obtains a key, then such key is considered a compromised key [14]. An enemy can gain access to a safe communication without the insight of sender or receiver by using the compromised key. The invader can decrypt or modify or change data by the negotiating key, and try to use the compromised key to calculate additional keys. Result is which could allow the attacker access to other secured communications or resources/assets. It is possible for an attacker to gain a key even though the process maybe a difficult and resource- demanding. For example, the attacker could take the sensors to execute reverse engineering job in order to know out the keys inside, and which could be represented in attack 9 shown in figure 3, also attacker may pretend to be a valid sensor node to fraud to agree on keys with other sensors.

3) *Man-in-the-Middle Attack:*

In man-in-the-middle attack [15], wrong messages are sent to the operator. This false message can take the form of a wrong negative or a wrong positive. This may cause the operator to take particular action, such as tossing a roller, when it is not required, or it may create the operator to think all is well and fine and he will not take any action when an action is required to be taken. For example, in Figure 3, attack 7 shows that the opponent sends V' to indicate a system change, however, V' is not the original actuate command or order. When the operator follows normal procedures and try to attempts to correct the problem, the operator's action could create an unfavorable event. There are number of variations of the modification and repeat of control data, which could influence the operations of the system. Attack 1, attack 3, attack 5 can also signify this kind of attacks.

4) *Denial-of-Service Attack:*

The final attack is called Denial of Service (DoS) attack [16] in which one of the network attacks that stop or avoid the genuine traffics or requests for network resources from being managed or reacted by the system. DoS attacks usually transmit a large quantity of data to the network to create busy handling the data and because of that normal services cannot be delivered.

The denial-of-service attack blocks normal working or use of the system. After gaining grant to the network of cyber-physical systems, the invader can always do any of the following:

- Stream a controller or the whole sensor network with traffic until a shutdown or hang occurs due to the overload.
- Send unacceptable data to controller or system networks, which causes irregular termination or behavior of the services.
- Block traffic, which results in a damage of access to network resources by official elements in the system. For example, in Figure 2, Attack 2 can represent that oppositions flood the whole sensor network with a very big amount of jamming data to chunk the normal network traffic, attack 6 can characterize that the adversaries send a enormous amount of invalid data to actuators to cause irregular closure of actuation process.

IV. CONTEXT-AWARE SECURITY STRUCTURE

In this paper we propose a context-aware security framework for cyber- physical security system

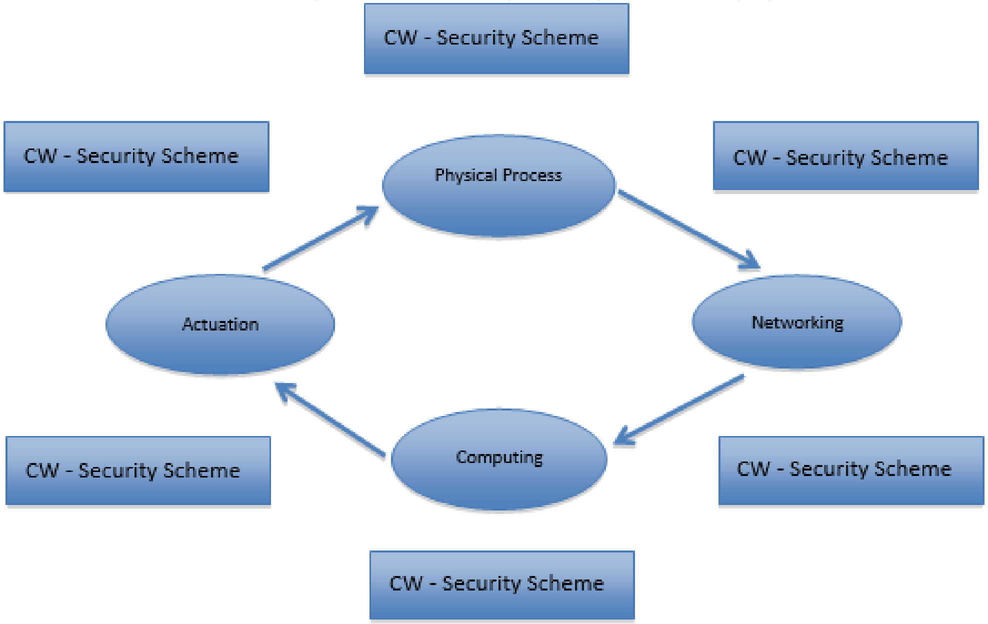

Fig. 3: The context-aware security framework

As shown in Figure 3, we formulate security-relevant framework information integrated into multiple security measurements such as , access control, authentication, key agreement protocol, encryption etc. Hence, security mechanism for cyber-physical system can be vigorously adapting to the physical environment by the support of context coupling. We call this kind of security mechanism context-aware security structure. Context is the position of environmental states and setting that determines an application's behavior and application event[18]. Context can be from various context information provider and can be changed form from many behavior. It is mainly categorized into four types: system (e.g. RAM, CPU, wireless network status, etc), user (e.g. behavior, places, emotion, medical history, etc), physical environment (e.g. light, temperature, weather, physical structure etc) and time. In our proposed structure, we mainly engage in security-related context which consist of the set of contextual attributes that can be used to describe the situation of an body, whose value affects the picking of the most appropriate control (trial) or the configuration of those controls to guard information and information system from illegal access, use, confession, disruption, modification or destruction in order to provide confidentiality, integrity and availability. When attacks are happening, the attack model and the opposition types can also be one of the contextual attributes.

Let's take an example of health related case, the doctor can be authorized to access his patients' physical condition records when available in hospital, while the location sensing data shows he is not available in hospital and located somewhere, but if the doctor wants to access the records, then the access control works attached with the changed context and reject this access. security framework can be represented as following method; the general workflow can be referenced in Figure 4:

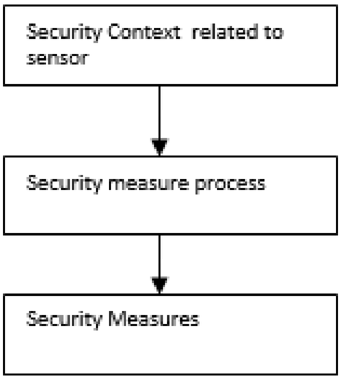

Fig. 4: Workflow of general context-aware security structure.

V. CONCLUSION

In this paper, we investigate the security challenges and issues of Cyber-Physical Systems and propose a security framework for CSPS. We hope that these challenges and issues bring enough motivation for future discussions and interests of research work on security aspects for CPS.

REFERENCES

[1] William Stallings, “Cryptography and network security: principles and practice”, Prentice Hall, 5nd Edition, ISBN-10: 0-13-609704- 9,2010.

[2] Nam Pham, TarekAbdelzaher, SumanNath, “On Bounding Data Stream Privacy in Distributed Cyber-physical Systems”, 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2010.

[3] 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.

[4] Leavitt, Neal, “Researchers Fight to Keep Implanted Medical Devices Safe from Hackers”, Computer, Volume 43, Issue 8, Pages: 11-14, August 2010.

[5] Daniel Work, AlexandreBayen 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.

[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] VanessaFuhrmans, “Virus Attacks Siemens Plant-Control Systems”, The Wall Street Journal, july 22, 2010. [8] J. Han, A. Jain, M. Luk, and A. Perrig, “Don’t sweat your privacy:Using humidity to detect human presence”, In Proceedings of 5th International Workshop on Privacy in UbiComp(UbiPriv’07), September 2007.

[8] Elinor Mills, “Hackers broke into FAA air traffic control system”, The Wall Street Journal, page A6, 2009.

[9] Jason Madden, Bruce McMillin, and AnikSinha, “Environmental Obfuscation of a Cyber Physical System - V ehicle Example”, Workshop on 34th Annual IEEE Computer Software and Applications Conference, 2010.

[10] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson,H. Shacham, and S. Savage. “Experimental security analysis of a modern automobile”, In Proceedings of the 31st IEEE Symposium on Security and Privacy, May 2010.

[11] KaiyuWan,K.L. Man,D. Hughes, “Specification, Analyzing Challenges and Approaches for Cyber-Physical Systems (CPS)”, Engineering Letters,issue3, EL_18_3_14, 2010.