Security Issues And Challenges For Cyber Physical System

R. Rajalakshmi, M. Shalini
Parisutham Institute of Technology and Science

Abstract:**In this paper, we investigate the security challenges and issues of cyber-physical systems. We abstract the general workflow of cyber physical systems, identify the possible vulnerabilities, attack issues, adversaries characteristics and a set of challenges that need to be addressed then we also propose a context-aware security framework for general cyber-physical systems and suggest some particular field in research field.**

Keywords- Cyber-Physical System, Security, actuation ,context-aware.

I. INTRODUCTION:

Cyber-Physical System aims at monitoring the behaviour of physical processes, and actuating actions to change its behaviour in order to make the physical environment work correctly and better. Commonly, a cyber physical system (CPS) consists of two major components, a physical process and a cyber systeTypically, the physical process is monitored or controlled by the cyber system,which is a networked system of several tiny devices with sensig computing and communication capabilities.The physical process involved may be a naturalphenomenon a man-madephysical system (e.g. a surgical room) or a more.However, as the interaction between the physical and cyber systems increases, the physical systems become increasingly more susceptible to the security vulnerabilities in the cyber system. For example, some hackers have broken into the air traffic control mission-support systems of the U.S. Now some hackers are also able to hack those medical devices implanted in human body which have wireless communication.In this year, hackers have designed a virus which can successfully attack Siemens plant-control system . consider an instance of gas leaking in a smart building, the cyber-physical system of the gas department must interact with the one which monitors the wounded person's health to accomplish the rescue mission.

II. GENERAL WORKFLOW OF CPS:

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

1.1.**Monitoring**: Monitoring of physical processes and environment is a fundamental function and it also give a feedback about CPS. .
1.2.**Networking:** This step deals with the data aggregation,diffusion. There can be much more than one sensor in CPS. These sensors can generate data in real-time,various sensors could generate much data which is to be aggregated or diffused for analyzers to processfurther. At the same time,different application are need to be interacted with networking communication.
1.3.**Computing**: This step is for reasoning and analyzing the data collected during monitoring to check whetherthe physical process satisfies certain pre-defined criteria.
1.4.**Actuation:** This step executes the actions determined during the computing phase. Actuation can actuate various forms of actions such as correcting the cyber behaviour of the CPS, changing the physical process. Fig 1 shows a general workflow of CPS. Let y represent the data acquisition from sensors, z the physical data aggregation in-network, u is the valid computed result of the physical system states which could advise controller to select valid commands, v is the control commands sent to the actuators.

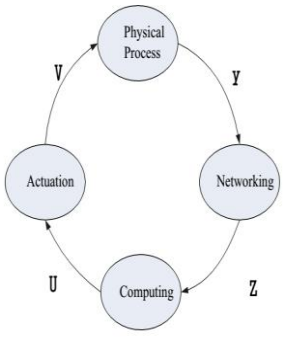

Figure 1. Abstraction of CPS

III. CPS SECRITY OBJECTIVES AND THREAT

3.1. Confidentiality

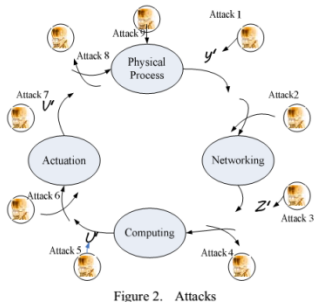

Figure 2. Attacks

3.1.1.Eavesdropping:
Eavesdropping refers to the attack t hat adversary can intercept any information communicated by the system .It is called passive attack that the attacker does not interfere with the working of the system and simply observes its operation. Eavesdropping also violates user privacy such as

a patient's personal health status data transferred in the system. In Figure 2 , attack 4 can represent the eavesdropping attacks on data aggregation processes.

3.1.2.Man -in-the-Middle Attack:

A man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each otherr. MITM attacks can be prevented or detected by two means: authentication and tamper detection. Authentication provides some degree of certainty that a given message has come from a legitimate source. Tamper detection merely shows evidence that a message may have been altered.

IV. CONTEXT-AWARE SECURITY FRAMEWORK

As Figure 3 shows, we make security-relevant context information incorporated into multiple security measurements such as authentication, encryption,key agreement protocol, access control and so on. We callthis kind of security mechanism context-aware security framework.

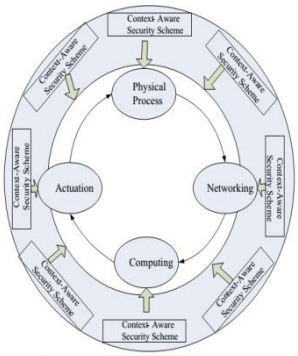

Figure 3. The context-aware security framework

Cyber Security: It includes communication securityand computing security. CPS is networked which not only allows them to form a network for data fusion &deliveryto back-end entities but also takecoordinated response actions.
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.

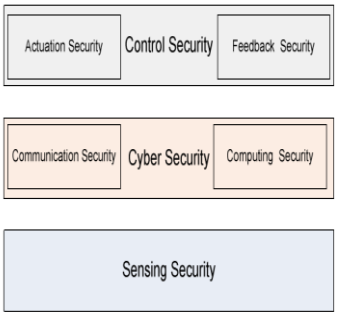

Figure 5. Main security aspects

V. FUTURE ENHANCEMENT:

The ability to interact with, and expand the capabilities of, the physical world through computation, communication, and control is a key enabler for future technology developments. . Finally we propose a new security framework for CPS and discuss a set of challenges and research problems that need to be resolved in the future .Opportunities and research challenges include the design and development of next-generation airplanes and space vehicles, hybridgas-lectric vehicles, fully autonomous urban driving, and prostheses that allow brain signals to control physical objects.

VI. CONCLUSIONS:

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

REFERENCES:

[1] Kaiyu Wan,K.L. Man,D. Hughes, "Specification,Analyzing for Cyber-PhysicalSystems(CPS)",Engineering Letters,2010.
[2] Elinor Mills, "Hackers broke into FAAWallStreet2009.
[3] Leavitt, Neal, "Researchers Fight to Keep Implanted Medical DevicesSafe from Hackers",August 2010.