An Introduction to Multilevel Security in Cyber Physical System

M.Sharada Varalakshmi
Associate professor, CSE
Department of Computer Science and Engineering
St.Peters Engineering College, Hyderabad, India

Abstract

Society has been facing considerable amount of challenges in recent years. Congestion of traffic, scarcity of energy, an increase in medical expenses and other problems have increased and turned for the worse and need urgent attention. These problems can be alleviated by applying technology and developing smart infrastructures. Smart infrastructures assimilate intelligence in everyday objects in order to improve the efficiency of certain elementary but crucial tasks. For example, a smart coffee pot detects decrease in temperature of its content and alerts its owner so that coffee is not unnecessarily reheated. This saves energy and reduces consumption of electricity. Similarly, traffic congestion can be reduced by incorporating sensors at specific location that sends signals to the base station about locations of congestion.

I. INTRODUCTION

The trend of developing such models has already begun. A survey in recent times found that a household has a minimum of 100 microprocessors within and a typical new car has at least 100 within it [M.J.Bass et al, 2002]. In fact, most microprocessors are embedded in those systems which are not actually computers [E.A.Lee, 2008]. This embedding technology has brought a revolution to develop miniature chips, sensor communications and processing platforms into larger systems to make smart infrastructures called Cyber Physical Systems. This provides real time monitoring and feedback services that are deeply embedded in physical processes [P.Tabuada, 2006].

The objective of Cyber Physical System is to monitor the physical system it is actually embedded in. It is a feedback system with human in the loop which actuates the actions to change its behavior if necessary. Cyber Physical Systems are designed as a combination of sensors, actuators, communications, and memory unit. For example, a pacemaker is built into a human's chest to monitor the behavior of the cardiac cycle and correct it in case of any extraordinary behavior [Q.Thang, 2008], or sensors distributed over a network in an automated processing unit or set the temperature data in an in-car network that can be monitored and controlled from the dash board where the information is displayed to the driver.

Cyber Physical Systems have a number of applications in various domains such as health management, traffic control, industrial automation units, power grids, infrastructures [B.Lai et al, 2002]. CPS has three primary characteristics:

- Environment Integration: CPS's are environmentally integrated systems – any environmental change involves change in the behavior of CPS and vice versa, examples such as medical devices, PDA's etc.
- Multiple abilities: CPS's are combined with diverse and heterogeneous capabilities. Sensors that are used for monitoring systems have limited capacity while those entities which manage them are more capable. For example, medical sensors such as RFID's or pace makers have limited capacity of storage but the base station is a computer which receives sensor data from multiple sensors across the network. This divergence is a direct bottle neck for communication, computing, processing and memory of CPS.
- Network Oriented: CPS are network coupled and require a communication channel integrated with a physical process to provide services [E.A.Lee, 2008]. For example, a sensor monitoring the traffic flow communicates with the base station about the traffic congestion in a particular area and thereby sends messages automatically to the drivers to take diversions.

Many issues need to be addressed in order to maintain safety, interoperability, sustainability and efficiency of CPS. These aspects need to be addressed at the development phase of the CPS. One of the most important factors to be considered during the development of CPS is security. The basic architecture and the components of the CPS are shown in figure1.1.

II. SECURITY FOR CPS

Security is the primary factor to consider in Cyber Physical System. In this section we discuss about the need for security to CPS, its workflow and challenges of CPS security.

A. Security need for CPS

Any security compromise of CPS can have great impact on the entire network. The mission

critical nature of CPS can make them more susceptible to targeted attacks. For instance, a pacemaker CPSs embedded in a human's chest cavity may be triggered to an untimely shock or to reveal the ECG data which makes them reveal the sensitive information of a patient's health [D.Halperin et al, 2008]. Similarly, a minor change in temperature or humidity of a manufacturing room of CPSs of an industrial automation unit may cause great damage to the entire information of the organization. Therefore, it is important to secure the sensitive information of the CPS system so that there are no malicious attacks. Intruders into CPSs systems and a minor change in any of the information may shutdown the entire unit. Today's world is rapidly depending upon the CPSs in automation, power grids, traffic monitoring, health care, etc. where care has to be taken to ensure their protection.

However, before we discuss the potential security issues of CPS, let us understand the flow of work of CPS. This helps us know the security issues in a CPS. CPS systems involves a number of entities such as, user groups to monitor and access the data , sensors in the network to collect data from sources, warehouse to store the collected data, a communication channel to report data to the store house, and actuators that can take actions on certain resources. The architecture shown in figure 1.1 gives a brief view about the smart-infrastructure of CPS, where it monitors the User groups, Network, Store house and provides access to the users for data mining.

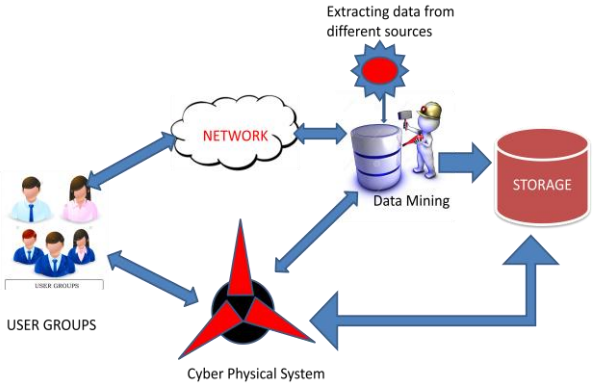

Fig: 1.1 Architecture of Cyber Physical System

B. Work flow of a Cyber Physical System

The workflow of CPS can be categorized into three major functions.

- Monitoring the network environment: The major task of CPS is to monitor the environment which it is embedded in. CPS has the ability to take feedback of the past and utilize it for future operations.
- Processing: The function of CPS is to analyze the acquired data while monitoring, and process it to meet certain pre-defined criteria. It takes certain corrective measures to ensure that certain criteria are satisfied. For example, the CPS can take certain corrective actions when rise in temperature with respect to certain scheduling algorithms for future use [Q.Tang, 2008].
- Actuation: This deals with determining the actions during the processing phase and executing them. This actually deals with the cyber behavior of the CPS to change its physical process. For example, authorization of information access in CPS.

The CPS work flow can be in any of these modes:

- Passive: In this mode, the CPSs are passive in nature, that is, they only monitor the environment, collect data, and process it e.g. medical RFIDs.
- Passively active mode: In this mode, CPSs monitor the environment and in case find any change in behavioral property; they execute change in its own behavior so that the property is satisfied. For example, change in the temperature more than the scheduled at specific spots may cause change in its behavior.
- Active mode: In this mode, CPS monitors their environment, and if any change in the property of physical environment, it immediately modifies its behavior to satisfy the property. For example, a HVAC system automatically changes its behavior whenever there is a change in the temperature in its environment.

C. Security Requirements of CPS

- Security to sensing data: CPSs are closely related to the environment they are embedded in. The data sensed must ensure validity and accuracy. Authentication is one measure to trust the sensed data [Feng Xie, Tianbo Lu 2013].
- Security to storage data: CPSs gather the data from hundreds of sensors in their environment and send it to the base computer. It must be ensured that the information system of the base computer is protected from malicious attacks for its sensitive information [A.A Cardenas et al, 2008].
- Security to Communication channel: Communication is one important aspect where security protocols have to be defined. It is important that there is an end to end communication both in inter and intra communication channels to ensure authentication of data [J.A. Stankovic et al, 2005].

Security to actuation of data: This ensures that actuation takes place in either passively active mode or passive mode. However, no actuation can take place without proper authorization [K.Venkata subramanian et al, 2008].

D. Challenges in Security of Cyber Physical System

Many challenges need to be considered for securing a Cyber Physical System. Some of them are:

Traditional security systems solely concentrate on cyber security whereas Cyber Physical systems are environmentally coupled where tampering sensor data in the environment may cause the Cyber Physical System malfunction.

Traditional security includes Confidentiality, Integrity, Authentication and Availability of the Cyber data of the entire system. CPSs also have similar applications of security along with security to each function of CPS such as, sensing, actuation, monitoring, storage and feedback, each of it has its own set of requirements for its functions and security. Unlike traditional security systems, CPS is environmentally coupled. Therefore, data of CPS is susceptible to man-in-the middle attacks.

CPSs are not deployed in a single and limited space. It is wide spread across the environment, and also many of the applications of CPS are monitored and operated by non technical people. So, it is important to have high degree of security on such systems.

III. MULTILEVEL SECURITY

Multi-level security is a concept proposed to protect the data from unauthorized users or networks [Nina Dobrinkova, 2010]. Generally in an organization, all users are not allowed to view all the data [Earl Boebert, TS Eliot, 2008]. There has to be certain hierarchy to view the data. This hierarchy of viewing the data is introduced as Multilevel Security (MLS). MLS has challenged the computer society by proposing two essential features. 1. The system must enforce restrictions regardless of the actions of system users or administrators. 2. Enforce these restrictions with incredibly high reliability[T.F. Lunt et al, 1990] The term multilevel arises from a defence sector where security is provided at different levels based on the classifications such as Confidential, Secret and Top secret.

We are aware that, the information related to defence, education, business industries, security organizations, paper institutions, finance sectors, National bilateral and multilateral related database systems hold information at different levels which are classified as Public, Confidential, Secret, and Top-secret. The data can flow at different levels, [Bell, LaPadula, 1976] it can be from “similar level” to “similar level” or from “lower level” to “upper level”.

The Multilevel security system is necessary for the present Cyber World because it ensures a subject to access an object of a particular classification appropriately [Bell et al, 2005].Protecting Highly Confidential and Confidential data is a major task in many organizations. If the access of information slides from lower level to upper level, organizations may face a legal or financial crisis. In order to overcome such crisis, the Information System must be tightly secured.

A. Need for Multilevel Security

Multi level security is first introduced in the military database Systems where the data is categorized into Confidential, Secret and Top Secret data [J.He, M.Wang, 1986].A layered security is given to the databases by using the technique of multilevel categories [D.E.Denning, 1986]. The usage of multilevel security gives Confidentiality to the data and also provides robust Access Control mechanism [P.Stachour, 1990].

Multilevel security is also essential because, protecting data at different levels ensures confidentiality. If access controls are applied adequately, it will be difficult for man–in–the middle attacks. Therefore, it becomes tedious for an intruder to access the Information System.

Protecting Secret and Top Secret data of information system is a major task for any organization, Multilevel Security is one solution for this [Han. J, Luk M, Perrig A 2007].

B. Challenges in Multilevel Security

Two major challenges of Multilevel Security that may incur are:

As technology has improved in communication and computers, there is an emergency need to protect data in information systems. Maintaining confidentiality of the system data is a major challenge in today’s world. Providing authorization is another major challenge of multilevel security.

Multilevel security features allow access to information with different sensitivity levels. Therefore data in the information system must be simultaneously stored, processed and provide the user with different security clearances, access permission and authorization. Providing authorization to access a system is not only challenging but also risky. In a smart infrastructure where users are of different categories, it is highly challenging, to maintain confidentiality and handling access permissions.

IV. MOTIVATION TOWARDS PAPER

Cyber Physical System is the most crucial area of National Cyber Infrastructure. Security threats to Cyber Physical System pose potential risk to health and safety to human lives, cause outrageous damage to environment and could impose dreadful loss on the economy. Industry surveys show that information security breaches are prevalent and more costly to handle in Cyber Physical systems. So, it is important to investigate the factors for security breaches. It is also important to maintain confidentiality and create a security mechanism to detect the intruders and protect the system from attacks. Also, protecting Secret and Top Secret data is a crucial task for any CPS. Surveys show that CPS systems are vulnerable to attacks due to its weak security and Access Control mechanism. The motivation towards the implementation of a Multilevel Security system (MLS) is to enhance the

access control mechanism by adding dynamic nature to it so that users can be monitored promptly to observe their movements in the environment. CPS being a real time system, handling the crisis dynamically is one major strand that has motivated us to take up this paper. These challenges are taken as motivation towards the development of Multilevel Security for a Cyber Physical System.

V. CONCLUSION

To meet our goals, a novel Multilevel Security system is designed and developed for an information system of a Cyber Physical System with key emphasis on categorization of data, storage randomization, encryption, user classification and Access Control.

It uses a design methodology for providing Multilevel Security for a CPS and experimentation is done using real time datasets. The results are validated for each of the methods by standard validation rules.

REFERENCES

[1] Adelstein, Frank, et al. Fundamentals of mobile and pervasive computing. Vol. 1. New York: McGraw-Hill, 2005.

[2] Ahn, Gail-Joon, and Ravi Sandhu. "Role-based authorization constraints specification." ACM Transactions on Information and System Security (TISSEC) 3.4 (2000): 207-226.

[3] Alfred J, Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.

[4] Amioy ,Kumar and Ajay Kumar. "Development of a new cryptographic construct using palmprint-based fuzzy vault." EURASIP Journal on Advances in Signal Processing 2009.1 (2009): 967046.

[5] Androutsopoulos, Ion, et al. "Learning to filter spam e-mail: A comparison of a naive bayesian and a memory-based approach." arXiv preprint cs/0009009 (2000).

[6] Anunciaçao, Orlando, et al. "A data mining approach for the detection of high-risk breast cancer groups." Advances in Bioinformatics. Springer Berlin Heidelberg, 2010. 43-51.

[7] Anyanwu, Matthew N., and Sajjan G. Shiva. "Comparative analysis of serial decision tree classification algorithms." International Journal of Computer Science and Security 3.3 (2009): 230-240.

[8] Ardagna, Claudio Agostino, et al. "Regulating exceptions in healthcare using policy spaces." IFIP Annual Conference on Data and Applications Security and Privacy. Springer Berlin Heidelberg, 2008.

[9] Clarke, Roger. "A major impediment to B2C success is... the concept'B2C'." Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet. ACM, 2006.

[10] Covington, Michael J., et al. "Securing context-aware applications using environment roles." Proceedings of the sixth ACM symposium on Access control models and technologies. ACM, 2001.

[11] Sandeep KS, Tridib Mukherjee, and Krishna Venkatasubramanian. "Criticality aware access control model for pervasive applications." Pervasive Computing and Communications, 2006. PerCom 2006. Fourth Annual IEEE International Conference on. IEEE, 2006.

[12] Han, Jiawei, Jian Pei, and Micheline Kamber. Data mining: concepts and techniques. Elsevier, 2011.