2012 12th International Conference on Computational Science and Its Applications

# Cyber Physical Systems Security: A Brief Survey

Qaisar Shafi
School of Electrical Engineering & Computer Science,
National University of Sciences and Technology (NUST), Islamabad, Pakistan
qaisar.shafi@seecs.edu.pk

*Abstract*— **Security challenges in Cyber Physical Systems necessitate solutions that are robust to threats posed especially when used in applications to monitor and secure critical infrastructures. In this work, we provide a decent bibliographic review of the existing literature on security of Cyber Physical Systems, identify key research challenges and discuss future directions on open research issues**

***Keywords-CPS; Security;***

## I. INTRODUCTION

Cyber-Physical System(CPS) are sensing, processing and communicating platforms, embedded in physical processes that provide real-time monitoring and processing. They have become common in many applications like health monitoring, smart vehicles and homes. CPS find applications in many real life real-time applications. The technology focuses on multi-domains such as embedded systems, communications, controls and computing to name few. and software is embedded in devices e.g. scientific instrumentation etc.

CPS mainly consists of two components, a physical process and a cyber system. The complete physical process is controlled and monitored by cyber system, which are small devices with basic wireless capabilities. The better interaction between physical and cyber system results in better performance and usability. CPS plays a major role in many applications including, medical devices, traffic control and safety measures, automotive systems, energy efficiency and environmental controls, instrumentation, critical infrastructures and many defense and smart systems.

The principle goal of CPS is to monitor behavior of physical process and actuate actions to change its behavior. All the components of CPS can be centralized or distributed. Key characteristics of CPS systems are environment coupling , diversity in capabilities and networked in nature.

This paper mainly focuses on the security requirements of CPS systems , security objectives and threats , major attacks on CPS and finally the discussion of the key areas where security of these systems are required and survey of the main security work that has been carried out in this domain.

## II. SECURITY OF CPS

### A. Need for CPS Security

The diverse capabilities of CPS help them to be used in mission critical processes. Any compromise in the security will result in worse consequences. CPS have ability to monitor the physical processes that are embedded in. so A data compromise data will result in loss of privacy and potential abuse of otherwise highly sensitive information. CPS are used in power-management so any malicious activity will result in socket bombing attacks. Finally, have the ability to actuate changes in the environment. Unauthorized activity will result in harm to the process.

### B. CPS security objectives and threats

#### 1) Confidentiality

Prevention of disclosure of information to unauthorized individual or system. Healthcare CPS requires the personal data of the patient to be transmitted confidentially to the doctor or medical device. This can be obtained by encrypting the data.

#### 2) Integrity

Refer to data or resource cannot be modified without authorization. Integrity is compromised as receiver receives false data and believe to be true.

#### 3) Availability

System or service must be available when it is needed. That is both physical controls and communication channels used to access must be available when it is needed.

978-0-7695-4710-7/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCSA.2012.36

*4) Authenticity*

The transactions and communications must be genuine. In CPS authentication refers to all the related process such as sensing, communication and actuations.

### C. Major Security requirements in CPS

*1) Sensing security*

Sensing security in CPS needs to be authenticated so that physical process can be trusted.

*2) Storage security*

Collected data required to be stored over for future access. Storage security involves developing solutions for securing stored data in CPS platforms from physical and cyber tempering.

*3) Communication security*

Need of developing protocols for securing both inter and intra-CPS communication for active and passive adversaries.

*4) Actuation control security*

No actuation can take place without appropriate authorization.

*5) Feedback security*

Estimation and control algorithms have to be studied for providing as in-depth defense against CPS.

### D. Major Attacks on CPS

*1) Compromised-key attacks.*

'Key' is the most secret information in security. Compromised key will result in the successful attack. Attacker can access any information with the help of that key. For example a attacker with the access of sensor node having a pre-shared key will result in the compromising of the security key.

*2) Man-in the middle attacks*

In these types of attacks false messages are sent to the operator, and they form a false negative or a false positive. Many common attacks like modification and replay attacks come in these domains.

*3) Eavesdropping*

In these attacks, attacker mainly interrupts the information communicated by the system. CPS is mostly affected by eavesdropping by traffic analysis and interrupting the data in the sensors and monitoring.

*4) Denial of service*

DOS attacks prevent the legitimate traffic to be transferred to legitimate communicating party. CPS are effected by DOS attacks in many ways like flooding the entire sensor network, controlled and abnormal termination of the services, most importantly blocking the legitimate traffic.

*5) Spoofing:*

The attacker poses as a legitimate part of a system and tries to take part in its operation. Once mounted successfully, the attacker can not only access information from the system, but also can modify or delete it, apart from introducing incorrect information.

### E. Major security concerns in CPS

Building a security mechanism for CPS is a great challenge because it involves both cyber and physical processes in integrated manner. This involves analysis form cyber vulnerabilities and their effects on physical system. Although such analysis cannot solve the problems, it provides a high level procedure to narrow-down the extent of security analysis that needs to be carried out on the cyber system in CPS. There are number of challenges involved in preventing, detecting and mitigating the attacks discussed in CPS.

*1) Prevention*

The interaction between cyber and physical systems result in a very large space to develop a prevention mechanism. Moreover existing security techniques may not be directly applicable due to additional constrains by CPS.

*2) Detection*

In distributed CPS, designing a mechanism is challenging. Sometimes a general attack may not correspond to the physical nature of the CPS.

*3) Mitigation*

It should coordinate with the physical mechanism of the CPS.

### F. Main CPS security Solutions

Much work has been carried out in designing the security architecture for these special types of systems. These solutions mainly focus on security of cyber systems and physical systems individually and interaction of both processes.

Some of these solutions are key agreement based and some focus on the access control aspects. Many solutions focus on all the security requirements of CPS including authenticity, confidentiality, authentication and availability.

Extensive work has been carried out on development of robust control and fault-tolerant systems in CPS.

In CPS context-aware security framework has also been presented in which they make security relevant context

information incorporated into multiple security measurement such as authentication , encryption , key agreement and access control etc.

### G. Key Establishment in CPS

Key establishment between sensors is the main security concern in CPS, the main categories includes:

*1) Pre-deployed:*

This technique is based on storing large number of keys in each sensor node before deployment.

*2) Communication based:*

This technique involves some of communication between entities and exchanging some information such as some Random Number (RN) or node ID.

*3) Public Key cryptography based:*

This technique involves use of public and private key pairs to distribute symmetric keys.

### H. CPS Security in important Applications

CPS Security concerns many important applications has been discussed e.g. Electric Power Grids, Smart grid infrastructures and Medical sectors. Much research issues have been discussed regarding security and privacy on creation of medical cyber physical systems. The attacker who potentially harm or penetrate a medical cyber physical system can pose a potential threat or induce harm to patients by reprogramming devices. In these types of attacks, adversaries can choose four classes of targets: patient, data, device and the interaction between internal network and medical cyber physical systems. Similarly, in other important application in this domain, electric power grids have many research challenges e.g. risk modeling, risk mitigation, coordinated attack defense, trust management and similar issues.

#### *Major Security Concern in a Smart GRID(SG)*

Authenticity

To make sure that the party are communicating with a genuine party authentication is the main security concern in SG.

Integrity

Another concern is that integrity of the data communicating in a SG should not be compromised.

Availability

The system should have the ability to recover from a attack. And the entire smart environment should be available to the parties when they need it.

Confidentiality

In a SG, confidentiality of the information stored or communicating between devices should have been a concern.

#### *Possible attacks on a Smart Grid(SG)*

Attack on authentication:

Millions of devices and systems connected to each other in SG offer many entry and exit points. This offers many potential points for an attacker. Authentication of data coming from a device and going to a device is a concern. Possible attacks on these points will make the SG vulnerable to source and destination authentication. A successful attack on authentication of SG devices, the attacker will be able to gain access on many control meters, and can shut down, reconfigure and disconnect many smart devices working in SG.

The control on these devices can result in malfunction of the entire environment. With incorrectly, decreasing or increasing the demand of electricity will result in many financial losses on consumers end (industrial demand of power/ consumers appliances etc. )

Attack on availability

Availability of all the communicating devices is major concern in SG. Captured device by an attacker e.g. power generator sensor or meter or any incorrect reconfiguration of device will result in total shut down or self destruction of the plant , which will result in non-availability of the resources to all parties. The consequence of this can be massive in the form of huge financial and customer losses.
Many similar DOS attacks on the smart environment are possible. The immense challenge for management will be a good recovery and business continuity plan to continue the basic business that is supply power to all consumers.

Attack on integrity

Integrity is also a major concern. The compromise to integrity of the data flowing in a SG can result in malfunctioning of the entire plant.

#### *Possible defenses and countermeasures:*

The possible attacks on a SG originate a need for an excellent security mechanism for this type of environment. For authentication related risks , there is a need of smart source and destination authentication mechanism that should able to cope with energy constraints in SG environment i.e small devices with limited processing capabilities. Moreover, to ensure availability of the resources, a basic recovery mechanism should be in place.

***Major Security concern in Oil and Gas Sector(OG)***

Authenticity

Like in Smart Grid, authentication is a main security concern in OG to make sure that communication is between legitimate parties.

Integrity

Compromise to integrity of the data is also alarming in OG sector.

Availability

The system should have the ability to recover from an attack. And the entire smart environment should be available to the parties when they need it.

*Possible attacks on OG*

Attack on authentication:

Millions of devices and systems connected to each other in OG sector offer many potential points for an attacker. A successful attack on authentication small devices working in an OG sector, the attacker will be able to gain access on many control meters, and can shut down, reconfigure and disconnect many smart devices working in SG.

Attack on availability

The non-availability of the resources in result of a successful attack e.g DOS can be devastating. The consequence of this can be massive in the form of huge financial and costumer losses. Many similar attacks are possible, need for a good recovery mechanism for the sector.

***Major Security concern in Navigation and Control***

The cyber physical systems working in navigation and control system have major security concern regarding authenticity, confidentiality and availability of the data. The wrong instructions to an unmanned aircraft, from a compromised control center can cause many lives and expensive infrastructure at risk. So it can be a major concern that the pilot should take instructions from an authenticated source.

The compromise to confidentiality and availability can also be destructive. The communication between craft and control center should be secure and system also should not be vulnerable to Denial of Services and similar attacks.

***Major Security concern in Water Resource Management (WRM)***

The automated WRM plays a major role in efficient management of water resources in a country. It deals with indications of water levels in different areas. The system takes decisions, which area required which amount of water resources. These systems are also based on CPS. The overall system consists of small sensing, communicating, storage and actuating devices.

Any security loophole in the system can be destructive. The incorrect water level indications in case of authentication failure between devices can result in floods and financial looses.

***Major Security Concern in Medical sector***

The last but not the least concern of CPS security is medical sector. This sector is also vulnerable to many security loopholes in the system. In this sector security is the concern from small devices attached to a patient e.g. a neonatal care unit, to cloud where all information related to a patient is residing, to a complete communication security from patient laying in on country and the doctor moving from one country to another with an hand held device for remote examining of the patient.

Any compromise to this storage and communication of information can result in death of the patient. Additionally wrong medication to a patient can result in long lasting disabilities and many concerns similar to that.

*I. Security Research challenges in CPS*

There are several areas that needs to be addressed in security of CPS systems. Major challenge is to attend hard problems rather than just fixing small vulnerabilities. The many issues regarding distributed computing systems needs to be addressed. The trust models need not to be hierarchical as different parts of the system able to achieve protection with main point of failure. Physical interactions in CPS must be modeled as data and control mechanism.

Security of sensors and actuators needs to be addressed. Techniques must be formed to detect tempering and possible modifications.

At last, there is a need of a overall system security architecture that supports both physical and cyber characteristics of CPS.

## III. CONCLUSION

In this paper, major security challenges and issues of CPS security are discussed. CPS has increasing security requirements due to their dual nature (physical and cyber). In order to design a security mechanism for these system these, aforementioned factors must be kept in mind.

## *REFERENCES*


[1] Alvaro A. Cardenas, Saurabh Amin, hankar Sastry, "Secure Control: Towards Survivable Cyber-Physical Systems," in Proc. of Intl. conf. on Distributed Computing Systems (ICDCS) - Workshops, pp. 495 - 500, 17-20 June 2008.

[2] A. Banerjee, K. Venkatasubramanian, and S. K. S. Gupta. Challenges of implementing cyber-physical security solutions in body area networks. April 2009. In Proc. of 4th International Conference on Body Area Networks.

[3] LIN Feng, SHU Shaolong, A Review on Cyber Physical Systems, JOURNAL OF TONG JI UNIVERSITY(NATURAL SCIENCE), 38(8), pp.1243-1248, 2010.

[4] [1] Lee, E., "Cyber-Physical systems - are computing foundations adequate?" In Position Paper for *NSF* Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, October 16 -17, 2006, Austin, TX.

[5] Tang, H., McMillin, B., "Security of Information Flow in the Electric Power Grid," *Critical Infrastructure Protection*, Springer Boston, pp. 43-56, 2007.

[6] J. Z. Li, H. Gao, and B. Yu, "Concepts, features, challenges, and research progresses of CPSs,"Development Report of China Computer Science in 2009, pp. 1-17.

[7] M. D. Ilić, L. Xie, U. A. Khan, *et al*. "Modeling Future Cyber-PhysicalEnergy Systems," in Proc. of Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008.

[8] T. T. Gamage, B. M. McMillin, and T. P. Roth, "Enforcing information flow security properties in Cyber-Physical Systems: A generalized framework based on compensation,"in Proc. of 34th Annual IEEE Computer Software and Applications Conference Workshops, 2010.

[9] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. In Proceedings of the VDE Congress,VDE Association for Electrical Electronic & Information Technologies, October 2004.

[10] A. A. C´ardenas, S. Amin, and S. Sastry. Research challenges for the security of control systems. In Proceedings of 3rd USENIX workshop on Hot Topics in Security (HotSec), San Jose, CA, USA, July 2008.

[11] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien. Roadmap to Secure Control Systems in the Energy Sector. Energetics Incorporated. Sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security, January 2006.

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

[13] P. Lukowicz, U. Anliker, J. Ward, G. Trster, E. Hirt, and C. Neufelt. Amon: A wearable medical computer for high risk patients. pages 133–134, October 2002. In Proceedings of IEEE 6th International Symposium on Wearable Computers.