IJCAT International Journal of Computing and Technology, Volume 1, Issue 6, July 2014
ISSN: 2348 - 6090
www.IJCAT.org

Security for Cyber-Physical Systems

Amey Vinayak Moholkar

University of Southern California
Los Angeles, CA90007, USA

Abstract - Cyber-Physical systems is an open system, which, integrate computing and communication with monitoring and/or control of entities in physical world. Use of CPS has increased many folds in recent years to automate and efficiently manage services. The real time nature and involvement in critical processes makes the security of CPS of paramount nature. Conventional security solutions for CPS focus on applying knowledge of traditional IT security to CPS environment. Though use of solutions from information security like authentication, encryption, access control etc. can be useful in CPS environment to some extent, we need to consider security solutions that take into consideration difference between IT systems and CPSs. Use of trusted computing offers many advantages, which can be incorporated in CPS to provide stronger security.

Keywords **- Cyber-Physical System, Security, Trusted Computing for CPS**

1. Introduction

Cyber-Physical Systems (CPSs) integrate computation with physical processes. In CPS, computation agents control the physical processes, with feedback loops where physical processes affect computations and vice versa. The Cyber-Physical system consists of two parts, the physical process and cyber system.

The cyber system is a set of devices with sensing, computing and communication capabilities embedded into them, which is used to control and monitor the physical process. This interaction between cyber and physical domains introduces new communication channels, which are not considered when one thinks of traditional IT system security.

The rest of this paper is outlined as follows. Section II describes the need for securing the CPS. Section III focuses on security issues of CPS, which are different from traditional IT systems. Section IV describes how traditional security goals apply to CPS. Section V surveys some existing solutions for securing CPSs. Section VI talks about incorporating trusted computing in CPS. Section VII outlines the roadmap for future research and Section VIII concludes the paper.

2. Need for CPS Security

Because of their diverse capabilities and environmental coupling, CPSs are often used for monitoring mission critical systems. Therefore any security compromise of the CPS can have dire consequences. Additionally this mission critical nature also makes them vulnerable to targeted attacks. Stuxnet, a highly targeted computer worm, designed to attack Siemen's industrial control system is an example of such an attack. CPS has the ability to actuate changes in physical domain they are part of [10]. Allowing unauthorized changes might harm the process itself. Attack against Maroochy Shire Council's sewage control system in Queensland, Australia is an example of how an attack on CPS can affect the physical domain of CPS. Consequences of this attack were - pumps not running when required, unauthorized modification of configuration data of pump station software and communication failure between the control center and the pumping stations. These problems caused the flooding of the grounds of a nearby hotel, a park, and a river with a million liters of sewage [9]. Further, CPS monitors physical processes they are part of. This makes them privy to sensitive information about the process. This information in hands of malicious entities might lead to disruption of the entire system [10]. As we are becoming more and more dependent upon CPSs for automated and efficient management of essential services, care must be taken to ensure their security.

3. Difference between traditional IT security and CPS security

While it is clear that emphasis on security of CPS is growing in recent years, much of the focus is on applying existing security mechanism of traditional IT systems to CPS. However to develop full proof security architecture for CPS we need to consider what is new and radically different in this field.

The **security goals** of traditional IT system and CPS differ. IT security gives more emphasis on protecting central servers than the edge clients. In CPS, however an edge device like PLC is not necessarily considered as

secondary to controllers or central data processing centers [8].The property of CPS that is most commonly bought up as a distinction with IT security is that frequent updates and software **patches is not very well suited for CPS** [3]. Considering the critical nature of some CPS, upgrading may require tedious advance planning of how to take system down. Problems due to this are not unheard of. On March 7 2008 a nuclear power plant in Georgia was accidently shutdown after software update of one of the computer, monitoring chemical and diagnostic data for plants control system. The software update rebooted the computer and it reset the data on the control system. Safety systems interpreted this lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods. As a result, automated safety systems at the plant triggered a shutdown [11].

Another property of CPS that differs from traditional IT system is **real time requirement** of CPS [3]. CPS includes decision-making agents, which needs to make decision in real time. Though availability is well-studied problem in information security, real time availability imposes more stringent operational rules than traditional IT systems. Many variants of CPS like SCADA (supervisory control and data acquisition) and industrial control systems are considered as hard real time systems [8]. Hard real time systems semantics impose rigid constraints on response time of a system. Failure to meet a deadline can lead to complete failure of the system and cause disastrous effects on physical process. This **timing aspect** differentiates CPS from traditional IT systems.

Sensor of CPS takes **input and feedback from physical environment**. This introduces new communication channels, which are not considered when one thinks of security of traditional IT systems [4]. Here an attacker does not need to break into the computer to cause the system to behave unexpectedly; instead series of coordinated physical events that are sensed by the system will do the trick.

Due to the physical nature, tasks and jobs performed by CPS and threads and processes within these **tasks/jobs are often needs to be interrupted** and resumed. The timing aspect and task interruption can make, use of conventional block encryption algorithm difficult [8]. Cyber-physical systems are often **geographically distributed**. Its components might be dispersed in the field where they lack appropriate physical security [4]. Such physical separation also makes it difficult to reset, or reload the software on a compromised device. Security solutions in such an environment must take into consideration compromised physical devices and its effect on the system. Constraints on **energy consumption and processing power** of devices in CPS such as sensors and actuators make deploying commercial IT software solutions in CPS environment difficult. Operation **environment of CPS is inherently uncertain**. Physical damage, component maintenance, weather conditions impose uncertainty, which defers CPS from traditional IT systems.

4. Security Goals and Requirements for CPS

4.1 Security Goals

In this section, I will describe how security goals of confidentiality; integrity and availability can be interpreted for cyber-physical systems.

Confidentiality is the ability to keep information secret from unauthorized users. Confidentiality in CPS must prevent an adversary from inferring the state of the physical system by eavesdropping on the communication channels between the sensors and the controller, and between the controller and the actuator. Integrity refers to the validity and trustworthiness of data. Integrity in CPS can therefore be considered as the ability to protect data sent and received by the sensors, actuators and the controllers from unauthorized modification. Availability refers to the ability of a system of being accessible and usable on demand [13]. The real-time constraint of CPS imposes strong requirements for availability of the system. The goal of availability in CPS is to keep system in operation state by preventing denial of service attacks [12].

4.2 Security Requirements of CPS

Fig. 1 illustrates security requirements for CPS. It consists of following five aspects [15]:

- **Sensing Security**: It deals with the integrity and accuracy of the data sensed by physical sensors.
- **Storage Security**: Is essential to prevent unauthorized modification of data stored in CPS.
- **Communication Security**: It is required to securing all communication channels within and outside the system from attackers.
- **Actuation Security**: It deals with authorization for performing actuation operation in CPS.
- **Feedback Security**: It is required to ensure that feedback loops to control system are protected in order to make accurate decisions.

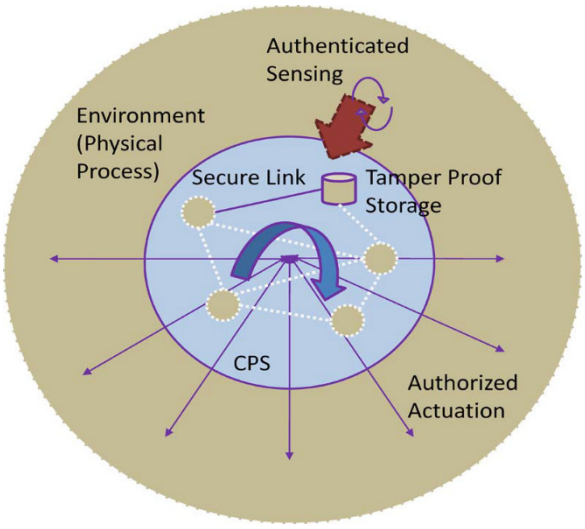

Fig. 1 Security Requirements for CPS [14]

5. Survey of Available Solutions

5.1 Solution from Information Security

Authentication tools can be used to prevent entities from impersonating another entity in the system. **Access control** can be used to avoid unauthorized access to system resources. It can be used to prevent unauthenticated entities from gaining access of the system and imposing restrictions on authenticated entities regarding what operations they can perform. For maintaining data integrity **digital signatures** or **message authentication codes** can be used [12]. **Timestamp** or **nonce** can be used to avoid replay attacks. Different **software tools** for detecting well-known vulnerabilities can be used to verify design and implementation of the system. Principles of **redundancy** can be effectively used in CPS. Redundancy means to avoid a single point of failure. Also principle of **least privilege** and principle of **separation of privilege** are effective in case of CPS. Considering, we can never rule out the possibility of successful attack, **intrusion detection and response systems** can be deployed in CPS environment [12]. Even though these systems have high rate of false positive and false negative (depending upon underlying design principles) it is better than having no security in place to detect and recover from an attack. **Cryptography** mechanisms can also be used to ensure data confidentiality and integrity. Considering the processing power of devices in CPS and their energy constraints security engineers suggest some lightweight cryptography approaches.

5.2 Cyber-Physical Security Solution (CYPSec)

CYPSec is a solution proposed in [16]. CYPSec solution takes into consideration the interaction of components with physical environment. It is based on the notion of using monitoring capacity of CPS to provide security. Complete explanation of CYPSec is out of the scope of this paper. Readers are referred to [16,10]. Some of the principal characteristics of CYPSec solution [10]:

- **Usability**: CYPSec uses environmental stimuli as a basis for security primitives. Because of this security and management abstractions need not be considered actively allowing designers of the system to focus on functional aspects
- **Emergence**: Along with required security functions of confidentiality, integrity and availability, CYPSec demonstrates additional allied properties, such as authentication and interoperability

5.3 Context-Aware Network Profiling

As explained in section V(A), intrusion detection systems can be effectively used in CPS environment. Context-aware network profiling is an approach suggested for creating accurate profiles of normal operations of SCADA systems. Conventional approaches for creating profile of normal behavior of CPS systems do not consider context of the messages passed on the network. Context-aware network profiling uses an approach that combines a quantitative and qualitative analysis of messages passed through the network. The qualitative analysis refers to monitoring parsed message types and parameter values, rather than coarse network statistics (such as flow-based statistics). The quantitative analysis refers to extracting statistical properties from observed message types and thus monitoring general trends of common operation [17].

6. Trust in CPS

Trust is the extent to which a trustor is willing to depend on a trustee to act dependably and securely in a given situation, with a feeling of relative security even though negative consequences are possible [2]. Trust is the confidence or reliance user of a system has about the integrity, availability, surety etc. about the performance of a system. Trusted application or system is one in which this confidence is justified i.e. trusted system is one that user believe will satisfy his/her expectations which is backed by substantial evidence [18]. Trustworthiness is the degree to which a system satisfies its users' expectations.

6.1 Principles of Trust

Dr. David Fisher has put forth following principles of trust [18]. These principles provide a framework for measuring and managing trust and trustworthiness of a system.

- Trust is essential. It is not possible to correctly interpret every probable aspect that can affect our system. Even rigorous validations cannot guarantee

trustworthiness. Hence for useful operation of any system some sort of trust on its design, implementation and use is essential.

- Trust must be evidence based and never absolute
  Confidence on functionality of a system should be based on evidence. Evidence can take many forms but predominantly depends on past performance or quality of a system we wish to trust.
- Trust should be partitioned by function and context
  Trust can and should vary within the system, depending on functionality under consideration, and context in which, it is evaluated.
- Trust must be confirmed dynamically
  Because we live in a dynamic world, the context and conditions of trust evaluation are guaranteed to differ from those in which the evidence of trustworthiness was generated [18]. Hence only dynamic confirmation can ensure that that trust on the system is justified.
- Trust should be proportional to the amount, quality and relevance of the evidence to the current context. While evaluating trust we must take into consideration only those evidences that are related to the current context.

6.2 Hardware Based Trusted Computing Platform

Hardware-based trusted computing platform provides a level of secure infrastructure that cannot be achieved by software implementations alone. Trusted Platform Module (TPM) is the basis of trusted computing. It is an international standard for secure crypto processor. It securely stores cryptographic keys, certificates and passwords. TPM provides following functionalities [19]

- An endorsement key that is a unique RSA key burned into the chip during production. This key can be used to establish that keys were generated in a TPM.
- Secure storage of HASH values of platform specific configuration information. These functions allow systems to do verifiable attestation of platform based on the chain of trust used while creating the HASH values.
- Secure storage of information using on-chip key pair generation with the help of hardware random number generator; asymmetric key encryption and decryption and digital signatures. Private keys created by TPM cannot be accessed outside TPM providing extra degree of security.

6.3 Benefits of Security Enabled by TPM

i. Secure network communication:
   In CPS, controller needs to make sure that sensors and actuators it is communicating with are authentic and communication channel is secure. Due to constraints on energy consumption and processing power, many times it is not advisable to implement complex processor intensive security mechanisms. TPM can prove beneficial in such circumstances [19]. TPM can
   - Use signatures to authenticate nodes, relying on the Common Criteria (CC) certification process to provide the assurance that the underlying processes do not allow for cloned signatures and hence cloned nodes
   - Generate session keys for communication using lightweight key exchange mechanisms.

ii. Secure Storage
   Many devices in CPS might store some potentially sensitive data. For example intermediate nodes of hierarchical sensor network, aggregates the data collected by sensors at the lower level and forward it to the upper level node. Data temporarily resides on such intermediate nodes. TPM can be used to encrypt all such information using the keys stored in TPM, which are not accessible outside

iii. Reliable peripheral identification
   In critical CPS, it is required that replacement to physical devices like sensors and actuators should be authentic. TPM can be used to attest these peripheral devices. For example, manufacturer can embed a TPM in a replacement device. System can then ask a newly added device to sign a random number to authenticate it.

iv. Secure firmware and software updates
   The devices of CPS might have to undergo firmware and software updates periodically. These devices could be dispersed over the field and manual upgrade of individual device might not be feasible. TPM can be used to verify the authenticity of a software or firmware upgrades provided by the manufacturer.

Apart from this use of TPM provides flexibility in terms of application areas in which it can be used. TPM uses standard cryptographic algorithms, which facilitates interoperability with systems, using different security mechanisms.

7. Roadmap for Future Work

Growth of security for Cyber-Physical System has been haphazard so far. It mainly involved applying the knowledge of traditional IT system security to solve immediate concerns and security vulnerabilities. Security of CPS needs to be built into the design of the system itself. Many CPSs are composed of ‘systems of systems’. While designing the security mechanism we need to consider this multilevel system design. Analysis of

vulnerabilities introduced at the boundary of such systems needs to be carried out in order to better understand and develop the threat model of the overall system. Most of the work on security of CPS is focused on securing the cyber domain and physical domain of CPS separately. Analysis focusing on interaction between these two domains should be carried out. As explained in section III, sensors and other devices of CPS are dispersed in the field and lack the physical protection. Threat models of CPS should take this into consideration and design security mechanisms, which tolerate loss of physical devices and make sure that acquiring such devices, will not leak any sensitive information to the attacker.

In above sections we have seen that incorporating trusted computing using TPM into the CPS offers many advantages. However, issues regarding managing root and chain of trust in distributed networks like CPS needs to be addressed. We talked about incorporating principle of least privileges and avoiding single point of failure. Research should be conducted for incorporating these factors into trust model of CPS. These trust models must not be monolithic, or even hierarchical, as different parts of a system must be able to achieve protection and provide availability for themselves, without a central point of failure or vulnerability [4].

Behavior of cyber-physical system is less dynamic as compared to traditional IT systems. For instance, many networked devices have static IP addresses; physical domain generally has well defined set of possible inputs to the control system etc. [17] Research regarding how to utilize these inherent properties of CPS to provide better security architecture should be carried out.
Finally, research on simple and lightweight mechanisms for providing strong isolation between different protection domains of CPS is needed [7].

8. Conclusion

Cyber-Physical systems have additional security requirements due to introduction of physical domain, stringent real-time availability restrictions and involvement in critical applications. Conventional solutions to security of CPS have largely applied traditional IT security model to CPS. Though effective in protecting against attacks on cyber domain, this approach does not take into consideration inherent difference between CPS and traditional IT systems. We need to consider this distinction before designing a security mechanism for CPS. Use of trusted computing in CPS, has its advantages. However issues regarding managing root of trust in distributed systems, developing a multilayer trust model supporting redundancy etc. are some of the factors that needs to be addressed.

References

[1] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee. Security challenges in next generation cyber physical systems. In Beyond SCADA: Networked Embedded Control for Cyber Physical Systems, November 2006.

[2] A. Jøsang, C. Keser, and T. Dimitrakos. Can we manage trust? In Trust Management, Proc. of the Third International Conference, iTrust 2005, Paris, France, May 23-26, 2005

[3] Alvaro A. Cárdenas Saurabh Amin Shankar Sastry. Research Challenges for the Security of Control Systems, University of California, Berkeley

[4] Dr. Clifford Neuman. Challenges in Security for Cyber-Physical Systems. Information Sciences Institute, University of Southern California.

[5] P. Tabuada. Cyber-physical systems: Position paper. In NSF Workshop on Cyber-Physical Systems, 2006.

[6] Annarita Giani, Adrian Perrig, Shankar Sastry, Challenges for Securing Cyber Physical Systems, Workshop on Future Directions in Cyber-physical Systems Security, DHS 23 July 2009.

[7] Dr. Clifford Neuman. Understanding trust and security in SCADA systems. In Beyond SCADA: Networked Embedded Control for Cyber Physical Systems, November 2006.

[8] Bonnie Zhu, Anthony Joseph, and Shankar Sastry, Taxonomy of Cyber Attacks on SCADA Systems, *Proceedings of CPSCom 2011: The 4th IEEE International Conference on Cyber, Physical and Social Computing*, Dalian, China, October 19-22, 2011.

[9] J. Slay and M. Miller. Lessons learned from the Maroochy water breach. In Critical Infrastructure Protection, volume 253/2007, pages 73–82. SpringerBoston, November 2007.

[10] Krishna Kumar Venkatasubramanian Security Solutions For Cyber-Physical Systems, Ph.D. Dissertation, Arizona State University December 2009.

[11] B. Krebs. Cyber Incident Blamed for Nuclear Power Plant Shutdown. Washington Post, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html, June 2008.

[12] Alvaro A. C´ardenas Saurabh Amin Shankar Sastry, Secure Control: Towards Survivable Cyber-Physical Systems, University of California, Berkeley.

[13] N. W. Group. Internet security glossary. http://rfc.net/rfc2828.html, May 2000.

[14] Ayan Banerjee, Krishna K. Venkatasubramanian, Tridib Mukherjee, Sandeep Kumar S. Gupta, Ensuring Safety, Security, andSustainabilityof Mission-CriticalCyber–Physical Systems, Proceedings of the IEEE (Volume:100 , Issue 1) Jan 2012

[15] Qaisar Shafi, Cyber Physical Systems Security: A Brief Survey, Computational Science and Its Applications (ICCSA), 2012 12th International Conference.

[16] K. Venkatasubramanian, S. Nabar, S. K. S. Gupta, and R. Poovendran, Cyber Physical Security Solutions for Pervasive Health Monitoring Systems, M. Watfa, Ed. IGI

Global, 2011, ser. E-Healthcare Systems and Wireless Communications: Current and Future Challenges.

[17] Dina Had˘ziosmanovic, Robin Sommer, Damiano Bolzoni, Pieter Hartel, Improving SCADA Security with Context-aware Network Profiling, University of Twente, Enschede, The Netherlands, International Computer Science Institute, Berkeley, Lawrence Berkeley National Laboratory, Berkeley.

[18] David A. Fisher, Principles of Trust for Embedded Systems, Technical Note CMU/SEI-2012-TN-007, March 2012.

[19] Embedded Systems and Trusted Computing Security, Trusted Computing Group News Letter