An Information Security Risk Assessment Framework for Cyber-Physical System

Keerti Dixit
Institute of Computer Science
Vikram University, Ujjain

Umesh Kumar Singh, PhD
Institute of Computer Science
Vikram University, Ujjain

Bhupendra Kumar Pandya, PhD
Institute of Computer Science
Vikram University, Ujjain

ABSTRACT
The term "Cyber-physical system" refers to a system that combines physical and cyber capabilities. It is a new field in the twenty-first century. CPS is in grave danger of being hacked. A well-designed CPS risk assessment will provide a comprehensive picture of the facility's security state and aid in the efficient deployment of safeguard resources. Despite the fact that standard IT system risk assessment is well-established, due to the significant differences between IT systems and CPS, a separate risk assessment method for CPS is required to address the developing security challenges. This paper highlights the security objective and challenges of CPS. In this research paper we have developed an Information Security Risk Assessment Framework for Cyber-Physical System.

Keywords
Cyber-physical System, Information Security Risk Assessment.

1. INTRODUCTION
Cyber-physical systems are the systems that combine the physical world with the world of information processing. CPS involves interaction between heterogeneous components that includes electronic chips, software systems, sensors and actuators. As a result, a CPS environment differs from and is more complicated than conventional environments. This is especially true because CPS is programmed to modify its strategy in real time to the present environment in response to the monitored situation [1].

CPS are similar to Internet-of-Things (IoT) systems, but they have more physical and computational coordination [2] [3]. Users, the physical environment, and a variety of hardware and software-based systems all interact with cyber-physical systems. Integration, interoperability, monitoring, and control of cyber-physical system components are all part of this. In contrast to stand-alone devices, CPS feature a chain of inputs and outputs linked to interacting elements. Furthermore, the application of CPS cannot be limited to a single field; rather their applications extend to almost every field [4]. These systems will enable advanced customisation of health care, traffic control, banking, and the smart grid, etc.

A CPS is characterized by the wide range of deployed technologies and a varying scale between such systems [5]. Computing devices, embedded systems, sensors, control units, and other devices that accomplish different tasks can all be deployed in a CPS. One CPS, for example, can mainly consist of a few sensor and actuator nodes for monitoring and adjusting the room temperature. A CPS, on the other hand, can evolve into a network of enormous heterogeneous and decentralised distributed subsystems that can, for example, conduct various autonomous activities on a solar energy plant [6]. CPSs have adaptive skills to handle both this complexity and changes in system scale. In most cases, the scale and diversity of deployed components define the complexity of a CPS. In addition, the majority of CPS use powerful feedback control technology. The ability to govern cyber-physical events in reaction to changes in the physical environment is referred to as feedback control [7].

2. SECURITY OBJECTIVES IN CYBER-PHYSICAL SYSTEM
Users' trust in cyber-physical systems must be acquired before they can be accepted in society. This trust can only be won if users are provided with acceptable security goals. Security goals aim to protect the system from threats and vulnerabilities while also reducing risk factors. The following is a list of some of the more common and important security goals:

2.1 Confidentiality
Confidentiality refers to the ability to keep information and data safe from unauthorised individuals or parties both inside and outside the system. Data and information confidentiality is maintained by encrypting stored and transferred data and restricting access to data storage [8]. Confidentiality is preserved in CPS by safeguarding communication channels against eavesdropping in order to prevent the system status from being deduced, as a result of eavesdropping [9].

2.2 Integrity
Integrity refers to the capacity to retain data in its original state and prevent unwanted changes. In other words, both outsiders and insiders who want to change the data must be kept out. As a result, when a destination receives wrong data, it treats it as correct. Integrity is assured in the CPS by detecting all possible attacks aimed at sabotaging the CPS's physical goals and altering data collected and relayed by sensors [10].

2.3 Availability
In general, this refers to the system's ability to deliver services and produce things on time. The capacity of all subsystems to perform effectively and do their tasks on schedule and as needed is referred to as availability [11]. In other words, availability assures that all CPS subsystems are operating properly by preventing all sorts of corruption, including hardware and software failures, power outages, and denial-of-service assaults.

2.4 Authenticity
This is the ability to ensure that all parties involved in CPS processes are doing what they are supposed to be doing. To

have an authentic and true CPS, authenticity must be realised in all subsystems and processes [8].

2.5 Robustness

The degree to which CPS can continue to function properly even in the face of minor disruptions is referred to as robustness. There are two types of failures: Limited failures have limited implications, while occasional failures have minor consequences that go away with time [9].

2.6 Trustworthiness

The degree to which people (e.g., owners, users, and individuals) can rely on the CPS to accomplish required activities within particular domain limits and under specific time limitations is known as trustworthiness [12]. To be termed a CPS that is both viable and trustworthy, the software, hardware, and data collected must all meet certain criteria.

3. SECURITY CHALLENGES IN CYBER-PHYSICAL SYSTEM

Cyber-physical systems are going through a revolutionary stage in their development, and as a result, they face numerous obstacles, the most important of which is security. CPSs, like traditional software systems, are vulnerable to cyber-attacks aimed at gaining internal data or disrupting data processing and storage [13]. Attackers attempt to gain access to the system, disseminate malicious code or malware, or gather sensitive data for their malicious intent, such as threatening organisations or masquerading a legitimate user by stealing identity data [14]. The functionality that governs the cyber-physical events in a system is disrupted when attacks on the 'cyber' element of a CPS are performed [15].

CPS must secure devices, data transmissions, applications, data storages, and actuation processes since they conduct multiple activities at various stages. These requirements are briefly described below:

3.1 Securing Access to Devices

The first challenge is securing access to devices. Unauthorized objects will get access and manipulate the system if authentication is not or is poorly provided [16]. As a result, neither the trustworthiness of any underlying binary codes nor the application-level implementation can be guaranteed.

3.2 Securing Data Transmissions

In order to detect impostors and harmful actions in CPS communication networks and restrict unwanted access, data transmission security is essential. Attackers, for example, try to intercept the physical properties of system power consumption and timing behaviours in order to examine the data delivered and received [16]. By conducting DoS attacks or disrupting the routing topology, some attackers want to interrupt networks [17].

Some terminal devices, which aren't full-fledged computers, lack advanced data processing, networking, and storage capabilities [18]. As a result, these gadgets are more vulnerable to cyber-attacks. Connectivity, which relies on open networking standards in Industrial Control System terminals, on the other hand, aids system performance and lowers operational expenses. While such terminals allow for more efficient and effective operation, they also expose the system to greater intrusions and malicious attacks, such as malicious code (malware), distributed denial of service (DDoS), eavesdropping and unauthorized access [19]. Another issue that contributes to vulnerabilities is the fact that the designing process is always confined in terms of processing time (speed), hardware resources, and power consumption. Furthermore, embedded systems are created by professionals with little experience with security challenges, and often place a greater emphasis on functionality, error correction, and performance than on security [20]. As a result, the system becomes vulnerable, potentially exposing sensitive information to unauthorised or unwanted users.

3.3 Securing Applications

The application layer brings together a variety of applications as well as security concerns. The issues of privacy protection that arise at this layer will not be addressed in the other layers where some security challenges do not occur. As a result, attackers can examine users' sensitive information, resulting in data leaks and privacy violations. Because this data may contain information about previous and current locations visited by users, location camouflage, anonymous space, and space encryption are some data protection approaches used at this layer. Furthermore, many applications in this layer interact on users' social lives, necessitating their protection [21].

3.4 Securing Data Storage

It's essential to keep confidential data in CPS devices safe. The majority of CPS devices, such as sensors, are small, wirelessly connected nodes with little resources [17]. Despite the fact that numerous software-based solutions use cryptographic approaches to encrypt data in such devices, they are insufficient due to memory constraints and the devices' limited processing capabilities. As a result, it is necessary to use lightweight security methods [22].

3.5 Securing Actuation

Actuation security means that any actuation activities must come from a reliable source. This will ensure that the feedback and control commands are precise and secure in the face of threats. [18].

Internet security risks will be involved as a result of using the Internet as a transmission layer in CPS connections. In general, rather than implementing simply the functioning security mechanism at each layer, security should be provided for the entire system as a single end-to-end security scheme [21]. Furthermore, significant memory needs and heavyweight computations are currently the fundamental criteria of any desirable security solution [23].

4. AN INFORMATION SECURITY RISK ASSESSMENT FRAMEWORK FOR CYBER-PHYSICAL SYSTEM

The Cyber Physical System's Risk Assessment Framework includes three phases of activity and a realistic approach for securing Cyber-physical Systems. The suggested Framework's purpose is to lessen the likelihood of security breaches, which entails figuring out what makes a system vulnerable.

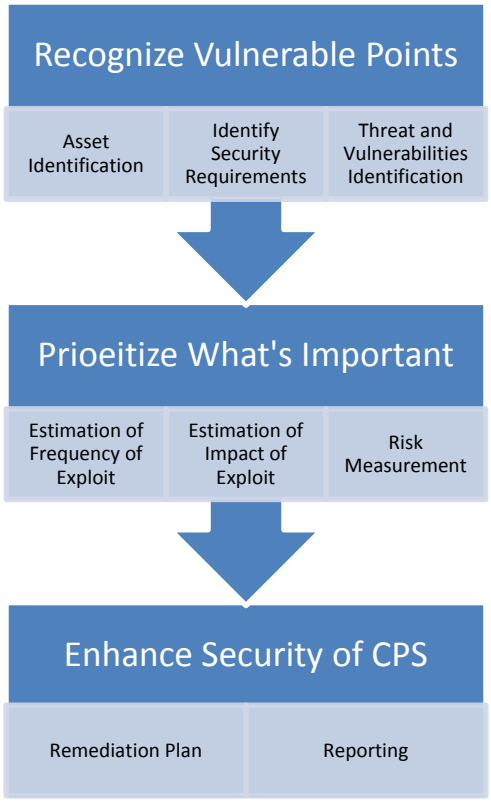

Figure 1: Information Security Risk Assessment Framework for CPS

Phase 1: Recognize vulnerable points

The goal of this phase is to identify weak points. The assets must be clearly specified according to the Risk Assessment Framework. The boundaries and content of the asset to be evaluated are defined in this step of the proposed framework. Information is considered an asset in the suggested framework. The scope of the risk assessment effort is then defined, and information necessary for establishing the risk is provided. This step requires data about hardware, software, data and information, network connections, and the system interface as input. Threat scenarios will also be constructed by outlining the most prevalent combinations of attack vector, attack goal, and attackers that could result in an asset being compromised.

Phase 2: Prioritize what's important

The second phase focuses on determining which locations provide the greatest risk. The likelihood of an attacker exploiting vulnerability is calculated in this phase. Exploit frequency will be determined.

The impact reflects the degree to which exploitation of a configuration flaw could directly affect a targeted system and the degree of loss of confidentiality, integrity, and availability. A quantifiable security risk level can be determined by the convergence of exploit frequency and impact.

Phase 3: Enhance security of Cyber-Physical System

The third phase focuses on developing a CPS repair plan and, ultimately, producing robust reporting to track recursive risk measurement actions.

5. CONCLUSION

Different sensors, data kinds, real-time generated data, process analysis, and numerous application interactions may be included in a Cyber-physical System. As a result, while connecting with other systems, it is vital to ensure that the system is secure. Using security mechanisms such as encryption techniques, authentication protocols, and steganography to improve CPS security will not eliminate all security risks. To some extent, such a solution could aid in the protection of the targeted system. However, when analysing security risk, every solution should take into account the application circumstances and context. As a result, improving application security will improve overall system security. In this work we have provides an overview of the Cyber-physical Systems, discusses the security objectives and security challenges of Cyber-physical Systems and developed an Information Security Risk Assessment Framework for Cyber-physical System.

6. REFERENCES

[1] L. Gurgen, O. Gunalp, Y. Benazzouz and M. Gallissot, "Self-aware cyber-physical systems and applications in smart buildings and cities," in Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 1149-1154). IEEE., 2013.

[2] R. Rajkumar, I. Lee, L. Sha and J. Stankovic, "Cyber-physical systems: the next computing revolution," in Design Automation Conference (DAC), 2010 47th ACM/IEEE (pp. 731-736). IEEE., 2010.

[3] L. Da Xu, W. He and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, 10(4), 2233-2243., 2014.

[4] J. Gubbi, R. Buyya and S. P. M. Marusic, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, 29(7), pp.1645- 1660, 2013.

[5] J. Wan, H. Yan, H. Suo and F. Li, "Advances in Cyber-Physical Systems Research.," KSII Transactions on Internet & Information Systems,, p. 5(11), 2011.

[6] M. E. Brak, S. E. Brak, M. Essaaidi and D. Benhaddou, "Wireless Sensor Network applications in smart grid," in International Renewable and Sustainable Energy Conference (IRSEC) (pp. 587-592). IEEE., 2014.

[7] B. Bordel, R. Alcarria, T. Robles and D. Martín, "Cyber–physical systems: Extending pervasive sensing from control theory to the Internet of Things," in Pervasive and mobile computing, 40, 156-184., 2017.

[8] Tawalbeh, L.A., Mowafi, M. and Aljoby, W. (2013) Use of Elliptic Curve Cryptography for Multimedia Encryption. IET Information Security, 7, 67-74. https://doi.org/10.1049/iet-ifs.2012.0147

[9] Rungger, M. and Tabuada, P. (2013) A Notion of Robustness for Cyber-Physical Systems.

[10] Lo'ai, A.T., Mehmood, R., Benkhlifa, E. and Song, H. (2016) Mobile Cloud Compu- ting Model and Big Data Analysis for Healthcare Applications. IEEE Access, 4, 6171-6180. https://doi.org/10.1109/ACCESS.2016.2613278

[11] Tawalbeh, L.A., Haddad, Y., Khamis, O., Benkhelifa, E., Jararweh, Y. and AlDosari, F. (2016) Efficient and Secure Software-Defined Mobile Cloud Computing

Infra- structure. International Journal of High Performance Computing and Networking, 9, 328-341. https://doi.org/10.1504/IJHPCN.2016.077825

[12] Kocher, P.C. (1996) Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Proceedings of CRYPTO, Santa Barbara, August 1996, 104-113. https://doi.org/10.1007/3-540-68697-5_9

[13] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," in IEEE Transactions on Signal and Information Processing over Networks, 4(1), 48-59., 2017.

[14] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo and F. Xie, "Cyber-physical System Risk Assessment," 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing., 2013. 169

[15] T. Lu, J. Lin, L. Zhao, Y. Li and Y. Peng, "A Security Architecture in Cyber-Physical Systems. Security Theories, Analysis, Simulation and Application Fields," IJSIA (International Journal of Security and Its Applications) 9 (7), 2015.

[16] Konstantinou C, Maniatakos M, Saqib F, Hu S, Plusquellic J, Jin Y. Cyber-physical systems: a security perspective, 20th IEEE Eur. Test Symp., pp. 1–8, 2015.

[17] Raza S. Lightweight security solutions for the Internet of Things, Mälardalen University Press Dissertations, Mälardalen University, Västerås, Sweden, 2013.

[18] Wang EK, Ye Y, Xu X, Yiu SM, Hui LCK, Chow KP. Security issues and challenges for cyber physical system, Proc. IEEE/ACM Int'l Conf. Green Comput. Commun. Int'l Conf. Cyber, Phys. Soc. Comput., pp. 733–738, 2010.

[19] Weiss J. Control system cyber vulnerabilities and potential mitigation of risk for utilities, White Pap. Juniper Networks, Inc., 2010.

[20] Hu W, Oberg J, Barrientos J, Mu D, Kastner R. Expanding gate level information flow tracking for multilevel security. IEEE Embed Syst Lett 2013;5(2):25–8.

[21] Jing Q, Vasilakos AV, Wan J. Security of the internet of things: perspectives and challenges. Wirel Netw 2014;20(8): 2481–501.

[22] Lu T, Xu B, Guo X, Zhao L, Xie F. A new multilevel framework for cyber-physical system security, pp. 2–3, 2013.

[23] Stankovic JA. Research directions for the internet of things. IEEE Internet Things J 2014;3–9. no. c.