Literature review on the threats and their countermeasures in cyber-physical systems CPS

Vikrant Singh
Department of Computing, Dublin City University (DCU) Glasnevin campus, The Mall, 630-, 672 Collins Ave Ext, Artane - Whitehall, Dublin 9

I. Introduction

CPS (Cyber-Physical System) is a concept that was first pitched by the National Aeronautics and Space Administration (NASA) in 1992 and these CPS systems are supposed to be revolutionary for the industrial system and they are supposed to be a foundation stone for the industrialization v4.0 [1] [4].

CPS defines as interconnected systems or networks which deals with physical outputs and inputs in real-time [3]. There are three core layers in CPS systems according to a framework named as Perception layer/physical layer with physical components of a CPS system such as sensors and actuators or any other physical device required for the system. The second layer is the Data transmission layer/Transmission layer which is a link between the perception layer and the application layer using communication networks and the third layer is the Application layer which provides services to the end-users [1] [2].

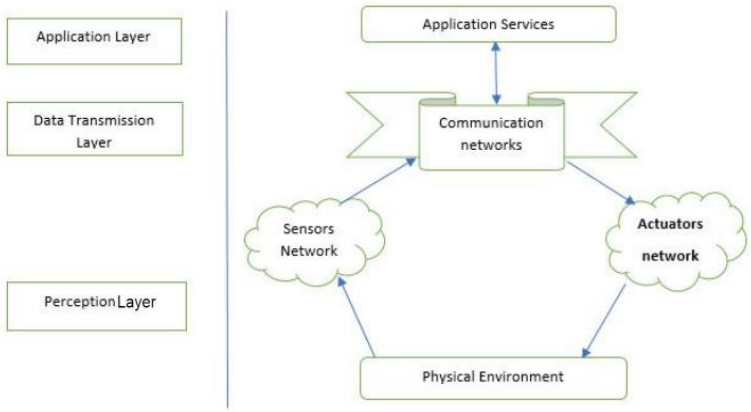

FIGURE 1 ARCHITECTURE OF CYBER-PHYSICAL SYSTEM [1] [4]

Although CPS systems are revolutionary, they are vulnerable to many attacks because of their large structure. The following literature review discusses some of the vulnerabilities and threats on the physical and cyber aspects of cyber-physical systems.

II. Classification of threats on CPS

Typically, there are two types of threats in cyber-physical systems first there are physical threats and the other is cyber threats. So, let's discuss them in the following section.

Physical Threats

As the CPS size grows the physical devices connected also increase rapidly and this leads to several physical attacks:

- **Infected Items:** includes the use of malicious devices such as DVD's and USBs and any other device to physically introduce malicious code [3].
- **Abuse of privilege** includes the harm caused by inner employees or authority which includes physical tampering of devices or any other unauthorized activity [3].
- **Physical Damage:** includes wire cuts, tampering and dialling and these things can lead to network problems and other losses [3].
- **Stalking, Fake identity and social engineering:** these attacks can happen separately and if the attacker is smart enough, he can use social engineering or stalking some employee to get a fake identity and can get access to the facility [3].
- **CCTV camera interception:** an attacker can get access to the camera footage by any remote or physical means and get to know the sensitive areas in the facility and can use this information in his favour to do some harm [3].
- **Key Hijacking:** most companies use a card system to provide access to employees and an attacker can steal this card or can social-engineering someone to get the key and can make multiple copies of the key to get full access to the area [3].
- **Physical Breach:** includes physical violation of the CPS system using illegal means and can result in loss of availability [3].

There can be more possible ways to attack CPS physically and all these attacks can cause loss of availability and productivity which can cause huge financial losses.

Cyber Threats

CPS systems are large infrastructures with many sensors and other devices which are using both public and private networks for data transfer and then use end applications to present the data. So, CPS are highly vulnerable to cyber-attacks and the following section discuss some of those attacks on three layers of the cyber-physical system and some attacks which are common to all three layers.

1) **Perception layer attacks:** The perception layer consists of devices like sensors, actuators, RFID and many other hardware devices called nodes and these nodes are in an unsecured and unsupervised environment and they are prone to many physical attacks like tampering and device failure. Moreover, not only physical attacks but these unprotected nodes are easy targets for attackers [1] [2]. Common attacks at the perception layer are information disclosure and tracking. Differential analysis, energy-exhaustion attacks, deception attacks, robust pole-dynamic attacks, covert and attacks, robust attacks and many more. Other than that, there are network attacks such as Actuator Enablement attacks (AE-attacks), Actuator Disablement attacks (AD-attacks), Sensor Erasure attacks (SE-attacks), and Sensor Insertion attacks (SI-attacks) [1] [2] and node-based attacks nodes capturing. False node, node outage path-based DOS and resonance which targets authenticity, integrity, authorization and availability [2].

2) **Data transmission layer attacks:** Attacks in this layer happen during the transmission of data between the other two-layer which are the perception and application layers. Capture packet and send a modification of packets using Man In The Middle attack is very common due to openness of wireless protocols and other than MITM there are many other such as traffic analysis using packet monitoring tools, black hole, flooding of packets cause DOS/DDOS, trap doors, sinkhole, direction misleading sinkholes, wormholes, wrong path selection, tunnelling and illegal access, routing loops, jamming wireless using jammers [2]. Moreover, any other attack in network devices and network layer in the OSI model can be possible depending on the type of network devices and protocols used for data transmission and even a small failure in the network leads to a huge loss of availability due to DOS/DDOS.

3) **Application Layer attacks:** This layer is used to interact with all the physical devices by using various applications and due to the versatile use of application technologies this layer is like an open field for attackers where they can play freely to find bugs and exploit them to get sensitive information. Web applications and mobile applications which are in wide use can be exploited for vulnerabilities for databases like SQL or MySQL injection, script insertion attacks like Cross-site scripting (XSS) to get user cookies, malicious code insertion and any other web application attack is possible. In addition to these attacks, there are common system flaws like buffer and stack overflows and malicious code insertion using remote access or local access like insertion of trojans and ransomware and also password cracking can be possible using brute force, dictionary or rainbow tables if proper access control is not implemented by the programmer. Moreover, there are social engineering attacks like phishing and eavesdropping (passive or active). Other than these vulnerabilities there are tons of other problems in these applications which are platform or technology-specific and can be exploited by the attacker.

III. Countermeasures for Different layers

1. **Perception layer:** Security parameters for the perception layer are authentication, confidentiality and trust management and the following are some common mechanisms to overcome them:

    - Certification must be used verification of data sent and received by devices [2].
    - Access control measures like privilege level must be controlled and proper +authentication methods should be implemented [2].
    - Encryption of data must be there to make it harder for an attacker to read and change data and a proper key management system should be implemented.
    - Sensor data should be shared protectively [2].
    - Continuous and regular environmental monitoring should be there so that any anomalies can be detected in the early stages [2].

- Secure routing protocols should be used, and we can use protocols like EIGRP and OSPF can be used because they have device authentication mechanisms and protocols like RIP should be avoided [2].

2. **Data Transmission Layer:** Security parameters for the transmission layer are integrity, availability, confidentiality, identity authentication which can be used following mechanisms to protect the CPS system to large extent.

   - Use robust routing protocols [2].
   - Hop by Hop data encryption should be applied [2].
   - Authentication and key agreement techniques between heterogeneous networks [2].
   - Network access control by setting privilege level accessing on routing devices [2].
   - Attack detection mechanisms like network-based Intrusion detection systems can be implemented along with firewalls to set policies for packet filtering and many other operations [2].

3. **Application layer:** Security parameters for the application layer are privacy, authentication and key agreements, authorization and also cloud security these days. Some counter-measures for the application layer are:

   - End to end encryption must be there for the applications [2].
   - P2P connection [2].
   - Application-based intrusion detection for detecting malicious code in the machines [2].
   - Proper user authentication and authorization mechanism [2].
   - Developers should use updated third party plugins and Softwares for designing the applications [2].

In addition to these basic mechanisms, there are many single and multilevel modern security that can be used to strengthen the security of CPS.

IV. Conclusion

Cyber-physical systems are multilayered integrated systems and they are the future of many industries. Although this large integrated environment provides a unique and productive structure CPS, this also comes which several security challenges and even many researchers are working on the security of the CPS and also there some effective security solutions already developed, since this is a new technology for the world and rapid technological advancements to CPS comes with new security challenges. So, there is still a wide area for research on the CPS regarding developing new security technologies and for the improvement in the currently available methods.

V. References

[1] L. Cao, X. Jiang, Y. Zhao, S. Wang, D. You and X. Xu, "A Survey of Network Attacks on Cyber-Physical Systems," in IEEE Access, vol. 8, pp. 44219-44227, 2020, doi: 10.1109/ACCESS.2020.2977423.

[2] Yosef Ashibani, Qusay H. Mahmoud,"Cyber physical systems security: Analysis, challenges and solutions", in Science Direct (ELSEVIER), vol. 68, pp. 81-97, 2017

[3] Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, Mohamad Malli, "Cyber-physical systems security: Limitations, issues and future trends", in Science Direct(ELSEVIER), vol. 77, pp. 103201, 2020

[4]Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang,"A survey on security control and attack detection for industrial cyber-physical systems", vol. 275, pp. 1674-1683, 2018