Paññāsāstra University of Cambodia

Sīla, Samādhi, Paññā (Pali)

Course: Academic Research Information Literacy

Instructor: Meas Rasmey

Research Paper: Cyber-Physical System Security: Protection for integrated systems.

Name: Thy Raksa

ID: 2223820

Cyber-Physical Systems (CPS) are networked systems in which the computational (cyber) part is tightly integrated with the physical components. That is, the computational components sense the state of the system and environment and then provide continuous feedback for controlling the system and actuating on the environment. Physical components include energy sources, transmission and distribution lines, loads, and control devices. Cyber components include energy management systems (EMS), supervisory control and data acquisition (SCADA) systems, and embedded implementations of control algorithms. The interplay of computational and physical systems yields new capabilities. The network is a key component in cyber-physical systems as it provides the backplane that guarantees timely transmission of the information (from the physical to the computational world) and of the commands (from the computation to the physical world).

Cyber-Physical Systems (CPS) are vulnerable to a range of cyber-attacks due to their integration of physical elements with networked computer systems. These attacks can disrupt essential infrastructure, pose safety risks, and compromise sensitive data. There are 3 common types of cyber-attacks on CPS. A DoS (denial-of-service) attack is a cyberattack that makes a computer or other device unavailable to its intended users. This is usually accomplished by overwhelming the targeted machine with requests until normal traffic can no longer be processed. With a DoS attack, a single computer launches the attack. This differs from a DDoS (distributed denial-of-service) attack, in which multiple systems simultaneously overwhelm a targeted system. One notable instance of a DoS attack in CPS occurred in Ukraine in 2015 and 2016, a group of hackers launched a cyber-attack against electric power stations in Ukraine – the first confirmed cyber-attack to take down an electricity power system. The cyber-attack was directed primarily at three regional electricity distribution companies (oblenergos). Attackers had used spear phishing emails containing Microsoft Office attachments that were infected with the BlackEnergy 3 malware, credential theft, VPNs access and other technical means to get access to the company's computers and SCADA systems. As a result, an interference with oblenergo`s system caused several outages that impacted approximately 225,000 customers in different regions and lasted several hours [18, p. III-IV]. A spoofing attack is a type of cyber-attack where an intruder imitates another legitimate device or user to launch an attack against the network. In other words, an attacker sends a communication from a device disguised as a legitimate device. Spoofing attacks are a widespread problem because they don't draw the same attention level as other attacks. While ransomware caught the attention of organizations around the world during the WannaCry attack, many organizations underplay the damage that can be caused by a successful spoofing attack. In 2018, attackers used IP spoofing as part of a large-scale Distributed Denial-of-Service (DDoS) attack on GitHub. The attack works by abusing Memcached instances that are inadvertently accessible on the public internet with UDP support enabled. Spoofing of IP addresses allows memcached's responses to be targeted against another address, like ones used to serve GitHub.com, and send more data toward the target than needs to be sent by the unspoofed source. The vulnerability via misconfiguration described in the post is somewhat unique amongst that class of attacks because the amplification factor is up to 51,000, meaning that for each byte sent by the attacker, up to 51KB is sent toward the target. A data breach is a cybersecurity incident that results in an unauthorized party's exposure or exfiltration of or damage to sensitive, confidential, private, or protected data. Data breaches are significant because they can lead to severe consequences for individuals (i.e., identity theft and financial loss, and organizations (i.e., reputational damage, legal repercussions, and financial penalties). The term data breach is often incorrectly used interchangeably with the term cyber-attack. The most notable difference between a data breach and a cyber-attack is that a data breach is a specific type of security incident resulting in compromised sensitive information. Importantly, a data breach, usually referring to digital information, encompasses data on physical media, such as paper documents, flash drives, laptops, mobile devices, and external hard drives. A cyber-attack can result in a data breach, but also includes other malicious activities, such as a distributed denial of service (DDoS) attack. In 2016, Yahoo revealed a 2013 data breach affecting over 1 billion accounts during its acquisition by Verizon. Later, it revised the figure to 3 billion accounts but clarified it wasn't a new security issue and notified all affected users.

The integration of IT and OT systems have created more connectivity between these two previously disparate environments, leading to improved efficiency, increased visibility and control over operations, and better decision-making capabilities for an organization. A prime example of IT/OT convergence are industrial internet of things (IIoT) devices, which involves the connection of physical devices, sensors, and machines to IT networks, often via the cloud. These devices enable data collection, remote monitoring, and analysis of performance — allowing critical infrastructure organizations to improve automation, predict maintenance, and make real-time decisions. Cyber-Physical Systems (CPS) face vulnerabilities that can be broadly divided into three categories: network, platform, and management vulnerabilities. Network vulnerabilities include weaknesses in security measures that protect communication channels, making CPS susceptible to man-in-the-middle, eavesdropping, replay, sniffing, and spoofing attacks, as well as communication-stack (network/transport/application layer) vulnerabilities. Additionally, attackers can exploit backdoors, launch Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks, and manipulate packets, which compromise both wired and wireless connections vulnerabilities involve flaws within the hardware, software, configuration, and database components, which can become entry points for cyber intrusions. Lastly, vulnerabilities stem from a lack of adequate security policies, guidelines, and procedures, which can lead to mismanagement and insufficient protection against cyber threats.

Securing CPS is not a straightforward task. For this reason, various existing solutions are mentioned and discussed in this section. Already existing testing tools have also been introduced. Cyber-Physical Systems (CPS) require a comprehensive approach to security due to their reliance on various integrated technologies and unique characteristics. According to the National Institute of Standards and Technology (NIST), ensuring security and trust between Internet of Things (IoT) and CPS requires a combination of multifactor security measures. These systems depend on critical attributes, including safety, security, privacy, consistency, dependability, resiliency, reliability, interaction, and coordination, which together create a well-designed and trustworthy CPS environment. Meeting these conditions is essential for establishing effective CPS mechanisms, with specific testing tools employed to evaluate the security of industrial control devices, as detailed in the work by Zhao et al. Security certifications are also available and are analyzed based on their varying characteristics. To maintain privacy, CPS systems must safeguard personal data, ensure transparency in data collection, and prevent unauthorized access. Dependability is achieved through adaptive behavior that ensures quality service, reliability, and safety, particularly when facing cyber threats or failures. Resiliency allows CPS to withstand and recover from accidents or attacks, as demonstrated in past incidents, such as the control breaches in Siemens plant systems and the U.S. Federal Aviation Administration's air traffic control system. Effective interaction and coordination are crucial for CPS to adapt to both cyber and physical changes over time, ensuring seamless operations between components. Operational Security (OpSec) enhances CPS effectiveness by securing information and assets, and involves steps like identifying critical information, analyzing threats and vulnerabilities, assessing risks, and applying countermeasures. System Hardening isolates critical applications from untrusted systems, enhances CPS integrity through trusted computing methods, and requires strong password policies, privilege management, and removal of outdated accounts to prevent remote attacks. Despite these advantages, CPS security measures may impact system performance, increase power consumption, introduce transmission delays, and incur higher costs and compatibility challenges. Maintaining security in Cyber-Physical Systems (CPS) is complex due to ongoing challenges in integration, security, privacy, and accuracy. CPS can be classified by criticality—safety-critical, where failure risks life and environment; mission-critical, where it affects functional objectives; business-critical, leading to financial loss; and security-critical, exposing security vulnerabilities. Cryptographic solutions, though limited by CPS constraints, secure communications against unauthorized access and attacks. Non-cryptographic methods include Intrusion Detection Systems (IDS), firewalls, and honeypots, which employ techniques like anomaly detection, rule-based analyses, and deception to monitor and protect systems. Honeypots, like HoneyBot, offer realistic decoys to capture attacker behavior and assess CPS security through high-fidelity simulations and frameworks like the Deep Detection Architecture (DDA), enhancing resilience against advanced threats.

In conclusion, the security of Cyber-Physical Systems (CPS) is a multi-faceted challenge requiring a holistic approach due to the interconnection of cyber and physical components and the critical nature of their applications. CPS systems, which often control infrastructure essential to public safety, are particularly vulnerable to cyber threats such as DoS/DDoS attacks, spoofing, and data breaches. Addressing these threats involves categorizing CPS by criticality to focus protection efforts on safety, mission, business, and security risks. Solutions include both cryptographic methods, which secure communications and data integrity, and non-cryptographic approaches, such as Intrusion Detection Systems (IDS), firewalls, and honeypots. Each method contributes to safeguarding these systems, though each brings trade-offs in cost, compatibility, and performance. The development of comprehensive, resilient security frameworks is essential to protect CPS from evolving cyber threats while ensuring they remain reliable and effective across diverse operational demands

Reference:

1. Claroty. (Jun 13, 2023). IT vs OT Security: Key Differences In Cybersecurity. Retrieved June 13th, 2023. https://claroty.com/blog/it-and-ot-cybersecurity-key-differences#:~:text=entire%20OT%20environment.-,2.,to%20CVEs%20and%20other%20 vulnerabilities.

2. GitHub. (n.d.). DDoS incident report. *GitHub News and Insights.* [March 1, 2018], from https://github.blog/news-insights/company-news/ddos-incident-report/

3. Ishaq, M., & Asghar, M. R. (2020). Cyber-physical systems (CPS): Vulnerabilities, threats, and countermeasures. *Frontiers in Information Technology & Electronic Engineering, 21*(7), 1014–1036. National Center for Biotechnology Information. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC7340599/#:~:text=In%20fact%2C%20CPS%20vulnerabilities%20are%20divided%20into,lack%20of%20security%20guidelines%2C%20procedures%20and%20policies

4. Investopedia. (n.d.). Denial-of-service (DoS) attack. *Investopedia.* [May 24, 2023], from https://www.investopedia.com/terms/d/denial-service-attack-dos.asp

5. Marisol García-Valls, ... Vicent Botti, in Journal of Systems Architecture, 2018 https://www.sciencedirect.com/topics/computer-science/cyber-physical-systems

6. National Center for Biotechnology Information. (2020). *Cyber-physical systems (CPS) security challenges: Classification and solutions*. National Institutes of Health. https://pmc.ncbi.nlm.nih.gov/articles/PMC7340599/#sec0029

7. SailPoint. (n.d.). Data breach. *SailPoint Identity Library.* Retrieved [Apr 30, 2024], from https://www.sailpoint.com/identity-library/data-breach#:~:text=A%20data%20breach%20is%20a,of%20service%20(DDoS)%20 attack

8. Tim Keary, Network Security and Administration Expert, 2023. A Guide to Spoofing Attacks and How to Prevent Them, https://www.comparitech.com/net-admin/spoofing-attacks-guide/

9. V. V. Muzyka, PhD Student, Assistant at the National University “Odesa Law Academy” 2020. ANALYSIS OF CYBER-ATTACKS ON UKRAINIAN POWER GRID SYSTEMS IN THE CONTEXT OF ARMED CONFLICT IN DONBAS. Indexcopernicus, https://journals.indexcopernicus.com/api/file/viewByFileId/1187881