16. SECURITY IN CYBER-PHYSICAL SYSTEMS

Adakhovskaya P.V.

Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Maksimchuk R.T. – Senior Lecturer

The structure and functionality of cyber-physical systems, their security concerns, and the models used to mitigate cyber threats are presented in this paper. The operation of a context-sensitive biometric security system is described.

Cyber-Physical Systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. CPS consist of the combination of various interconnected systems with the ability to monitor and manipulate real Internet of Things (IoT) applications. These highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances, such as smart manufacturing, smart home, smart health care, smart cars, smart traffic management, ecological system, defense, etc. CPS play a key role in industry sectors, enable smart applications to operate accurately in real-time with potential to create innovative applications that affect multiple economic sectors [1].

The ability of CPS to recognize and adapt to environmental changes permit them to effectively manage physical operations. This allows CPS to perform four key functions: monitoring, networking, computing, and actuation. These functions work together to enhance automation, optimize performance, and improve decision-making applications [2].

Given their important role in different fields, CPS must implement strict security measures. Integrity, confidentiality and authenticity are the three criteria for security. Integrity ensures that data remains unchanged without proper authorization, preventing misinformation. Confidentiality restricts access to confidential information, protecting it from unauthorized access. Authenticity ensures that communication and data

exchange are carried out between legitimate parties, which ensures identity verification at every stage, including detection, data transfer and activation [3].

Several models have been developed to enhance CPS security:

- game theory is used to model the interaction between attackers and defenders, helping to develop strategic security measures;
- petri nets visualize sequences of cyberattacks, revealing vulnerabilities in the system architecture;
- stochastic games include probabilistic models to analyze how attackers adapt to a dynamic security environment.

These models help security professionals assess risks and take targeted countermeasures.

One of the most promising approaches to ensuring security is a context-sensitive biometric security platform. This platform integrates authentication, encryption, key management, and access control to ensure security. This increases the degree of protection through the use of real-time functions such as one-time passwords and biometric verification, forming a multi-factor authentication system. Context-dependent factors, including location, system status, lighting, temperature, and time, further strengthen security mechanisms. For example, if access is requested from an unusual location, the system may grant conditional access using additional verification rather than outright denial.

The context-sensitive biometric security system is widely used in important sectors such as healthcare, finance, and smart infrastructure. Its ability to continuously monitor user behavior helps identify anomalies and eliminate security threats in real time.

As consumer protection services continue to evolve and expand in various industries, ensuring their safety remains a top priority. The integration of cyber-physical elements into these systems opens up both opportunities and challenges, especially with regard to data protection and access control. By implementing such adaptive security mechanisms, organizations can enhance the resilience of consumer protection systems by protecting confidential information from increasingly sophisticated cyber threats.

References:

1. *Why Cyber-Physical Systems are important toward future and what are the current issues in it? [Electronic resource]. - Mode of access: https://medium.com/@jeevanandamj/why-cyber-physical-systems-are-important-toward-future-and-what-are-the-current-issues-in-it-7c58f6531312. - Date of access: 10.03.2025.*

2. Pham et al. (2010) N. Pham, T. Abdelzaher, S. Nath, "On Bounding Data Stream Privacy in Distributed Cyber-physical Systems", 2010 IEEE.

3. Neal (2010) L. Neal, "Researchers Fight to Keep Implanted Medical Devices Safe from Hackers", Computer, Volume 43, Issue 8, Pages: 11-14, August 2010.