RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Architecture Of Information Security Threats in Cyber-Physical Systems

By

Alexandra Yuryevna Bokovnya
Ph. D. in Law Faculty of Law, Department of Criminal Law
Kazan Federal University Kazan, Russia (Russian Federation)
Email: kafedra.ksu@yandex.ru
ORCID: https://orcid.org/0000-0002-6395-0893

Ildar Rustamovich Begishev
Doctor of Law, Senior Researcher Kazan Innovative University named after V.G. Timiryasov Kazan, Russia (Russian Federation)
Email: begishev@mail.ru
ORCID: https://orcid.org/0000-0001-5619-4025

Abstract

The article discusses in detail the physical attacks and cyber-attacks against cyber-physical systems, the main failures in cyber-physical systems, the basic requirements for the security of cyber-physical systems, the issues of ensuring the security of cyber-physical systems and the legal aspects of cyber-physical system security. Cyber-physical systems suffer from a variety of security and privacy issues that can reduce their reliability, security, effectiveness, and possibly hinder their widespread deployment. Accordingly, it is necessary to apply a number of measures to enhance their safety while maintaining the required performance. It is determined that the prospects for the development of legislation in the field of liability for harm caused with the participation of cyber-physical systems are associated with the changes in digital technologies and the evolution of social norms.

Keywords: cyber-physical system, vulnerability, information security, cyber threat, physical threat, robot, robotics, artificial intelligence

Introduction

Despite their many advantages, cyber-physical systems (hereinafter referred to as CPS) are subject to various threats, attacks and challenges to cyber or physical security. This is due to their heterogeneous nature, their reliance on private and sensitive data, and their large-scale deployment. Thus, intentional or accidental impact on these systems can lead to catastrophic consequences, making it critical to take strong security measures.

Materials And Methods

The theoretical research of scientists on various issues of cyber-physical system security served as the material for this work. The methodological basis of the study is a set of methods of scientific knowledge, including abstract-logical, comparison and correlation analysis.

Security aspects of cyber-physical systems

The researchers analyzed various aspects of CPS safety:

– various CPS safety objectives have been listed and discussed in the writings by T.M. Chen, C. Miller, C. Valasek, E. Bou-Harb, N. Sklavos, I.D. Zaharakis[1];
– possible ways of CPS safety provision were proposed in the work by A. Humayed, J. Lin, F. Li, B. Luo [2];
– the problems of CPS safety provision are covered in the works by H. Yoo, T. Shon[3];
- the problems with data storage, as well as the issues related to the vulnerability of the operating system are presented in the studies by H. Ye, X. Cheng, M. Yuan, L. Xu, J. Gao, C. Cheng, J.S. Kumar, D.R. Patel, R.E. Johnson, O. Kocabas, T. Soyata, M.K. Aktas, S. Lai, P. Cordeiro, A. Hasandka, N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, M. Martin[4].

All authors note that CPS are integrated into critical infrastructures (intelligent grids, industry, supply chains, healthcare, military, agriculture, etc.), which makes them an attractive target for attacks on security for various purposes, including economic, criminal, military, espionage, political and terrorism too. Thus, any CPS vulnerability can be used to carry out dangerous attacks on such systems. Confidentiality, integrity and availability are at risk, which can cause serious damage to CPS users and owners.

Security Threats to Cyber-Physical Systems

In this regard, the authors consider it important to identify the main threats, vulnerabilities and attacks to the CPS security, discuss the advantages and limitations of existing security solutions in order to determine the requirements for a secure, reliable and efficient CPS environment. Most researchers are of the opinion that CFS systems require innovative security solutions that can provide a good balance between security level and system performance[5].

CFS security threats are proposed to be divided into cyber threats and physical threats, in combination they can lead to cyber-physical threats[6].

The main focus of Industrial IoT security is on cyber threats rather than physical threats for many reasons. 6 The reason for this is the dynamic development of information technologies. Electronic attacks are now easier to organize and carry out from any device, unlike physical attacks that require physical presence and physical tools. Such attacks are difficult to minimize and overcome if there are no specialized defensive countermeasures. Cyber threats have been studied in detail in a number of works[7].

Main types of cyber threats to the security of cyber-physical systems

There are different types of cyber threats:

– use of a wireless network: a hacker is required to know the structure of the system and thus makes it possible to use its wireless capabilities to gain remote access or control over the system to disrupt the system[8];
– "jamming the system" - in this case, attackers usually seek to change the state of the device and the expected operations in order to cause damage by triggering the waves of deauthentication or wireless jamming signals, which will lead to the device failure[9];
- intelligence. This threat is implemented through the distribution of malicious software, which leads to the violation of data confidentiality due to the limitation of traditional security measures[10];

– the attempt to get remote access. This threat is implemented through the launch of malicious programs, power outages, the artificial creation of network failures, as well as through the theft of industrial data and industrial espionage[11];
- information disclosure. Hackers can reveal any personal information by intercepting communication traffic with wireless hacking tools[12], violating both privacy and confidentiality[13];
- unauthorized access. In this case, attackers attempt to gain unauthorized access through a logical or physical disruption of the network and obtain sensitive data, which leads to confidentiality breach[14];
- interception. Using this technique, hackers can intercept private conversations using existing or new vulnerabilities, which also leads to confidentiality breach[15];
– use of GPS. Using this technique, hackers can track a device or even a car using navigation systems (GPS)[16].

Main types of physical threats to cyber-physical system security

CPS systems have recently been developed into the industrial area through the introduction of advanced metering infrastructure and neighborhood networks, as well as data meter management systems to maintain the stability of CPS in industrial areas[17]. In this regard, the following physical threats to the CPS may arise:

- physical damage. They may be applied to non-essential facilities as these stations are well staffed and effectively secured through the implementation of access control, authorization and authentication mechanisms such as usernames and passwords, access cards, biometrics and video surveillance. Less secure targets are at stake - smart meters that need to be tamper-proof by relying on fault detection or even host-based intrusion detection[18];
- failure of one of the important subsystems due to the attacker's fault. For example, in the event of a severe damage to the smart grid, a complete blackout in large metropolitan areas can occur for several hours[19].

The authors also identify certain types of physical threats that are potentially possible for the CPS:

- spoofing. It consists of disguising the identity of a trusted entity by an unknown malicious source. In this case, attackers can tamper with the sensors, for example by sending misleading or false measurements to a control center;
- sabotage. It consists of intercepting legitimate communication traffic and redirecting it to malicious third parties or disrupting the communication process. For example, attackers can sabotage physically exposed CPS components on the power grid to cause a service disruption or even a denial of service, resulting in a complete or partial power outage;
– failure or denial of service. Attackers can physically tamper with any device to disrupt service or change configuration. This can have serious consequences, especially when using CPS in medicine;
– tracking. Since the devices are physically open, an attacker can gain access to this device[20].

Main vulnerabilities of cyber-physical systems

Besides, it is necessary to identify the main vulnerabilities of the CPS, which can be targeted by the above-mentioned threats.

A vulnerability is defined as a security hole that can be exploited for industrial espionage purposes (intelligence or active attacks). Therefore, vulnerability assessment

includes the identification and analysis of existing weaknesses in the CPS, as well as the determination of appropriate corrective and preventive actions to reduce, mitigate or even eliminate any vulnerability. [21]

In fact, CPS vulnerabilities fall into three main categories:

1. Network vulnerabilities. These include weaknesses in security controls, in addition to compromising open wired or wireless communications and connections, including mediation, eavesdropping, replay, sniffing, spoofing, and the communication stack (network, transport, application layer). [22]
2. Platform vulnerabilities: include hardware, software, configuration and database vulnerabilities.[23]
3. Management vulnerabilities. They include the lack of security procedures.[24]

Causes of Vulnerabilities in Cyber-Physical Systems

Vulnerabilities arise for many reasons. However, there are three main reasons for their appearance:

1. Assumption and isolation: it is based on the "security through obscurity" trend in most CPS projects. Therefore, the focus here is on designing a reliable and secure system, considering the implementation of the necessary security services, without assuming that the systems are isolated from the outside world.
2. Increase of connection number. Increase of connection number increases the attack surface. The introduction and use of open networks and open wireless technologies increases the level of this vulnerability.
3. Heterogeneity. CPS systems include heterogeneous third-party components that are integrated to create CPS applications. This has led to the fact that CPS has become a multi-vendor system, where each product is subject to different security issues.[25]
4. Espionage. CPS systems are also subject to surveillance attacks, mainly through the use of spyware (malware) that gain covert access and go unnoticed for many years, with the main task being to eavesdrop, steal and collect confidential data and information.
5. Homogeneity of CPS. Similar types of CPS suffer from the same vulnerabilities that, once exploited, can affect all devices in the immediate vicinity. [26]

Summary

Thus, CPS vulnerabilities can be of three types, including cybernetic, physical, and in combination they lead to a cyber-physical threat. It has been determined that the minimization of technological security risks of cyber-physical systems will significantly enhance their progressive development and progress.

Acknowledgements

This paper has been supported by the Kazan Federal University Strategic Academic Leadership Program.

References

T.M. ChenSurvey of cyber security issues in smart grids Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II, 7709, International Society for Optics and Photonics (2010), p. 770-790;

C. Miller, C. ValasekA survey of remote automotive attack surfaces Black Hat USA, 2014 (2014), p. 94; E. Bou-HarbA brief survey of security approaches for cyber-physical systems 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE (2016), pp. 1-5;

N. Sklavos, I.D. ZaharakisCryptography and security in internet of things (IoTs): models, schemes, and implementations 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE (2016), pp. 1-2

Humayed, J. Lin, F. Li, B. LuoCyber-physical systems security-a survey IEEE Internet of Things J., 4 (6) (2017), pp. 1802-1831

H. Yoo, T. ShonChallenges and research directions for heterogeneous cyber–physical system based on IEC 61850: vulnerabilities, security requirements, and security architecture Future Gener. Comput. Syst., 61 (2016), pp. 128-136

H. Ye, X. Cheng, M. Yuan, L. Xu, J. Gao, C. ChengA survey of security and privacy in big data Communications and Information Technologies (ISCIT), 2016 16th International Symposium on, IEEE (2016), pp. 268-272;

J.S. Kumar, D.R. PatelA survey on internet of things: security and privacy issues Int. J. Comput. Appl., 90 (11) (2014); R.E. JohnsonSurvey of SCADA security challenges and potential attack vectors Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, IEEE (2010), pp. 1-5;

O. Kocabas, T. Soyata, M.K. AktasEmerging security mechanisms for medical cyber physical systems IEEE/ACM Trans. Comput. Biol. Bioinform., 13 (3) (2016), pp. 401-416;

C. Lai, P. Cordeiro, A. Hasandka, N. Jacobs, S. Hossain-cKenzie, D. Jose, D. Saleem, M. MartinCryptography considerations for distributed energy resource systems 2019 IEEE Power and Energy Conference at Illinois (PECI), IEEE (2019), pp. 1-7

K. Zhao, L. GeA survey on the internet of things security 2013 Ninth International Conference on Computational Intelligence and Security, IEEE (2013), pp. 663-667;

R. Khan, S.U. Khan, R. Zaheer, S. KhanFuture internet: the internet of things architecture, possible applications and key challenges 2012 10th International Conference on Frontiers of Information Technology, IEEE (2012), pp. 257-260;

Y. Geng, C.-m. Rong, C. Veigner, J.-T. Wang, H.-B. ChengIdentity-based key agreement and encryption for wireless sensor networks J. China Univ. Posts Telecommun., 13 (4) (2006), pp. 54-60;

Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. QiuSecurity of the internet of things: perspectives and challenges Wirel. Netw., 20 (8) (2014), pp. 2481-2501

T. Sommestad, G.N. Ericsson, J. NordlanderSCADA system cyber security-a comparison of standards Power and Energy Society General Meeting, 2010 IEEE, IEEE (2010), pp. 1-8

R. Alguliyev, Y. Imamverdiyev, L. SukhostatCyber-physical systems and their security issues Comput. Ind., 100 (2018), pp. 212-223

E. Bou-HarbA brief survey of security approaches for cyber-physical systems 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE (2016), pp. 1-5;

F.M. ClevelandCyber security issues for advanced metering infrasttructure (AMI) Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, IEEE (2008), pp. 1-5;

A.R. Metke, R.L. EklSmart grid security technology Innovative Smart Grid Technologies (ISGT), 2010, IEEE (2010), pp. 1-7

S.Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al.Comprehensive experimental analyses of automotive attack surfaces. USENIX Security Symposium, San Francisco (2011), pp. 77-92

M. Rushanan, A.D. Rubin, D.F. Kune, C.M. SwansonSok: security and privacy in implantable medical devices and body area networks 2014 IEEE Symposium on Security and Privacy (SP), IEEE (2014), pp. 524-539

K. Deconstructing flame: the limitations of traditional defences Comput. Fraud Secur., 2012 (10) (2012), pp. 8-11; B. Miller, D.A survey SCADA of and critical infrastructure incidents Proceedings of the 1st Annual Conference on Research in Information Technology, ACM (2012), pp. 51-56

P. McDaniel, S. McLaughlinSecurity and privacy challenges in the smart gridIEEE Secur. Priv., 7 (3) (2009), pp. 75-77

B. Miller, D.A survey SCADA of and critical infrastructure incidents Proceedings of the 1st Annual Conference on Research in Information Technology, ACM (2012), pp. 51-56

D. Halperin, T.S. Heydt-Benjamin, K. Fu, T. Kohno, W.H. MaiselSecurity and privacy for implantable medical devices IEEE Perv. Comput. (1) (2008), pp. 30-39

Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. MullenFortino, S. Park, A. Roederer, et al.Challenges and research directions in medical cyber-physical systems Proc. IEEE, 100 (1) (2012), pp. 75-90

D. Halperin, T.S. Heydt-Benjamin, K. Fu, T. Kohno, W.H. MaiselSecurity and privacy for implantable medical devices IEEE Perv. Comput. (1) (2008), pp. 30-39

R. Brooks, S. Sander, J. Deng, J.Automotive system security: challenges and state-of-the-art Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, ACM (2008), p. 26

H. Zeynal, M. Eidiani, D.Intelligent substation automation systems for robust operation of smart grids 2014 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA), IEEE (2014), pp. 786-790

T.M. Chen, J.C. Sanchez-Aarnoutse, J. BufordPetri net modeling of cyber-physical attacks on smart grid IEEE Trans. Smart Grid, 2 (4) (2011), pp. 741-749

S.M. Amin Securing the electricity grid Bridge, 40 (1) (2010), pp. 19-20

E. Byres, J. LoweThe myths and facts behind cyber security risks for industrial control systems Proceedings of the VDE Kongress, 116 (2004), pp. 213-218

J. MoteffRisk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences Library of Congress Washington DC Congressional Research Service (2005)

B. Zhu, A. Joseph, S.A taxonomy of cyber attacks on SCADA systems2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, IEEE (2011), pp. 380-388

V. Sridharan Cyber security in power systems, Georgia Institute of Technology (2012) Ph.D. thesis

S. Amin, G.A. Schwartz, A. HussainIn quest of benchmarking security risks to cyber-physical systems IEEE Netw., 27 (1) (2013), pp. 19-24

E. IasielloCyber attack: a dull tool to shape foreign policy 2013 5th International Conference on Cyber Conflict (CYCON 2013), IEEE (2013), pp. 1-18