SECTION XII.
AUTOMATISATION ET INSTRUMENTATION

DOI 10.36074/logos-01.10.2021.v1.27

ANALYSIS OF INDUSTRIAL INTERNET OF THINGS VULNERABILITY TO CYBERATTACKS

ORCID ID: 0000-0002-2590-7085 **Yevsieiev Vladyslav**
Doctor of Engineering Science, Professor,
Department of Computer-Integrated Technologies, Automation and Mechatronics
Kharkiv National University of Radio Electronics

ORCID ID: 0000-0002-9931-9964 **Nataliia Demska**
Candidate of Engineering Science, Associate Professor,
Department of Computer-Integrated Technologies, Automation and Mechatronics
Kharkiv National University of Radio Electronics

UKRAINE

Currently, the widespread implementation of Industry 4.0 concepts has led to the emergence of complex Cyber-Physical Production Systems (CPPS), which are based on the paradigm of "digital production" [1]. Digital production is a mirror image of physical processes in virtual space. For this to exist, it is necessary to develop one information eco-system that combines: sensors, Programmable Logic Controller (PLC), Supervisory Control And Data Acquisition (SCADA) / human-machine interface (HMI) and allows you to implement a single Manufacturing Execution System (MES). Industrial Internet of Things (IIoT) is a network that allows you to unite all industrial facilities in order to solve problems: increasing equipment productivity, reducing material and energy costs, improving quality, optimizing technological processes [2]. As a result, multiple flows of information appear for many different operations, from signal processing to optimization, visualization, cognitive and high-performance computing. To deal with a huge amount of data, industrial clouds are used, they are located in an area remote from the main production. Thus, it inevitably continues to expand and use the growing computing power available to operators via smartphones and laptops [3]. Cybersecurity - protection against unauthorized access and theft of business information and valuable knowledge in digital form. Before finding a solution for cybersecurity breaches, it is necessary to synthesize existing knowledge about possible cybersecurity threats targeting different levels of IIoT, as well as the consequences and countermeasures. Ramjee Prasad, Vandana Rohokale analyzed methods of cyber-attacks on Machine to Machine (M2M) [4]. Based on this, we can select a Network Layer through which an attack can be carried out using the following methods, which are shown in the figure 1.

M. Lezzi, M. Lazoi conducted an analysis of publications and research in the areas of cybersecurity for Industry 4.0 [5]. In which the possibility of carrying out cyberattacks at the SCADA / HMI, MES level through the Internet of Things (IoT) was highlighted. Considering the complex publications, one can distinguish Application Layer (fig. 2) and attack methods [6-10].

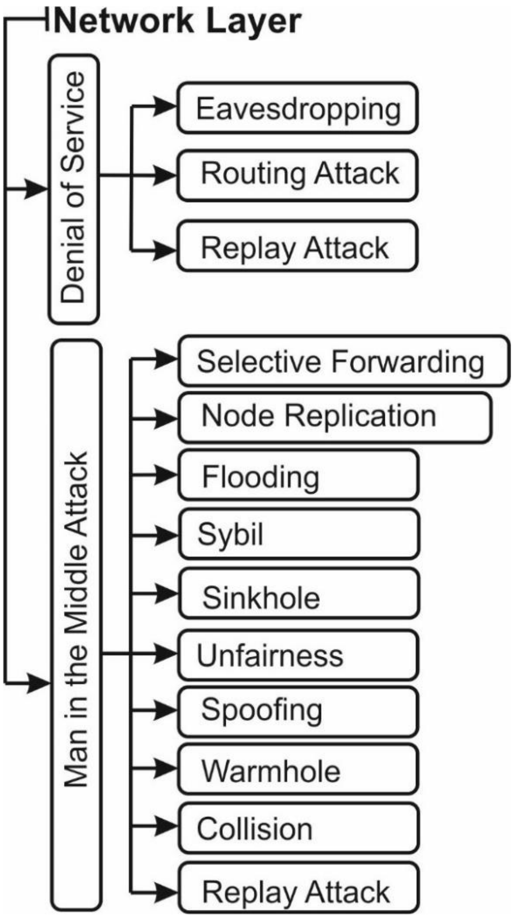

Fig. 1. **Cyberattacks targeting network layer of IIoT**

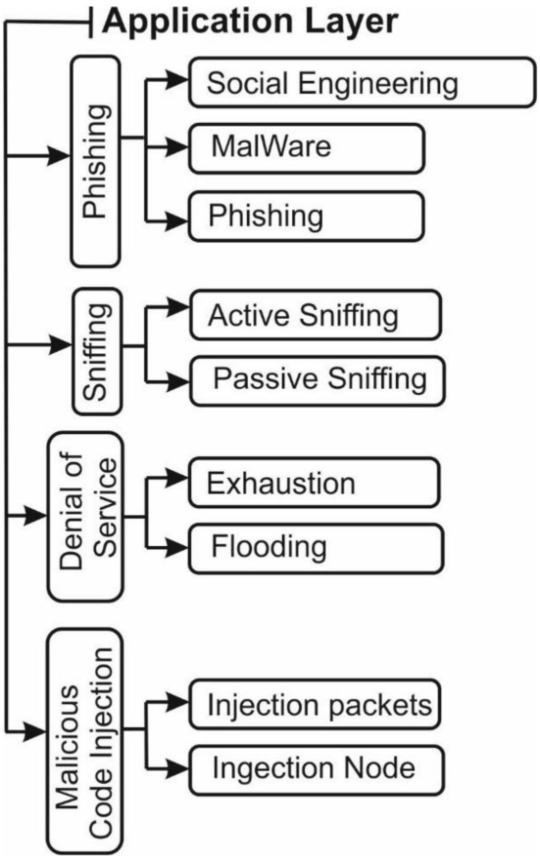

Fig. 2. **Cyber-attacks targeting Application layer of IIoT**

Conclusions. Vulnerability analysis showed that Application Layer is one of the more vulnerable levels, due to the large influence of the human factor, also due to the use of open Internet networks, when working remotely. As a result, the authors consider the need to develop new methods of hardware and software protection against information leakage.

References:

[1] Nevliudov, I., Yevsieiev, V., Demska, N. i Novoselov, S. (2020) Розробка програмного модуля оперативно-диспетчерського контролю виробництва на базі кібер-фізичних систем керування, *Сучасний стан наукових досліджень та технологій в промисловості*, (4 (14), pp 155-168. doi: 10.30837/ITSSI.2020.14.155.

[2] Nevliudov, I., Yevsieiev, V., Maksymova, S., & Filippenko, I. (2020). Development of an architectural-logical model to automate the management of the process of creating complex cyber-physical industrial systems. Eastern-European Journal of Enterprise Technologies, 4(3 (106), 44–52. DOI: 10.15587/1729-4061.2020.210761.

[3] Mamoona Humayun, NZ Jhanjhi, Muhammad Nabil Talib, M H Shahd, G. Sussendran. (2021). Industry 4.0 and Cyber Security Issues and Challenges. Turkish Journal of Computer and Mathematics Education Vol.12 No.10. p. 2957-2971.

[4] Ramjee Prasad, Vandana Rohokale. (2019). Internet of Things (IoT) and Machine to Machine (M2M) Communication. Cyber Security: The Lifeline of Information and Communication Technology pp 125-141. DOI: 10.1007/978-3-030-31703-4_9.

[5] M. Lezzi, M. Lazoi, and A. Corallo. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework, Computers in Industry, 103, 97-110.

[6] D. Pancaroğlu. (2018). An Analysis of the Current State of Security in the Internet of Things, International Conference on Cyber Security and Computer Science (ICONCS'18), Safranbolu, Turkey.

[7] R. Von Solms, N. J. Van. (2013). From information security to cybersecurity, computers & security, 38, 97- 102.

[8] M. Akin, S. Sağiroğlu, Gelişmiş Sürekli Tehditler, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi , 10 (1) , 1-10, 2017.

[9] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. (2012). Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD- based approach, In Resilient Control Systems (ISRCS), 5th International Symposium, 55-62, 2012.

[10] C. K. Chen, Z. K. Zhang, S. H. Lee, and S. Shieh, Penetration Testing in the IoT Age, Computer, 51(4), 82-85, 2018.