Cybersecurity of Industrial Internet of Things

Oksana Linkevych, Nataliia Bozhok
National University of Food Technologies, Kyiv, Ukraine

Introduction. Industrial Internet of Things (IIoT) security is an important question when designing ready-made solutions. The problem is the lack of methodological recommendations for building secure IIoT solutions.

Materials and methods. A lot of IIoT consist of different levels: hardware, networks, and accessories. The latter requires special attention, as we can give hackers a wide entry area and require use cloud, mobile and web applications.

Results. There are specialized businesses and security services to provide encryption, hash functions, authorization, authentication and so on. According to the triad of key principles of information security, any data should be protected based on confidentiality, integrity and availability [1;2;3]. Since in most cases IIoT solutions require remote access to manage and handle large amounts of information, there is a need for comprehensive protection, building a threat model, and examining existing IoT-targeted viruses (including Miral, Stuxnet and others) [1;2]. Cryptography is mandatory for IIoT, because it helps ensure interoperability, protects the firmware and authentication process. Often, IIoT devices have a limited computing power and low memory, complicating the use of sophisticated cryptographic algorithms that require more resources than the devices can provide. Encryption can be divided into three levels: symmetric encryption, public-key encryption, cryptographic hashing. Security measures must be taken into consideration when designing solutions in terms of IIoT, and the approach must be comprehensive and cover all aspects, from hardware to cloud [1;2;3].

The analysis of modern research has shown that there is a short list of security measures for decision-making in IIoT sphere and it requires a constant updating. As a result, we have developed a list of advice for IIoT security. The main of these tips are presented below. At first, it is important to use the latest versions of operating system and libraries with all the necessary patches. We are of the opinion that a user should choose the original password randomly. Besides, all IP ports have to be closed by default. The user should also sign with certificates, encrypt, protect his firmware, software images and use hardware that supports security features such as secure runtime, TRMs and non-executable address spaces. We highly recommend using trust root and securing boot to ensure that the genuine software runs on the customers` devices. We think that it is useful for IT experts to provide manufacturers with a mechanism to fix bugs and vulnerabilities in production systems. In order to do this, the software architecture must be multi-tasking and up-to-date.

Conclusions. The existing methods of protection of IIoT solutions were analyzed and the urgent measures were identified to avoid the threats. The mentioned key actions are planned to be formulated as recommendations for IT experts as well as professional users.

References.

1. Perry Lee Internet of Things for Architect 2018 [Електронний ресурс]. – Режим доступу: https://www.amazon.com/Internet-Things-Architects-communication-infrastructure/dp/1788470591
2. Industrial Internet Consortium.Industrial Internet Security Framework [Електронний ресурс]. – Режим доступу: http: // www.iiconsortium.org/IISF.htm.
3. Industrial Internet Consortium. Industrial Internet Reference Architecture(IIRA). [Електронний ресурс]. – Режим доступу: https://www.iiconsortium.org/IIRA.htm.