INTERNET OF THINGS TRAPS IN NATIONAL AND INTERNATIONAL CYBER-SECURITY SOLUTIONS

Andras TOTH

ABSTRACT

This paper presents the different standards and protocols to build a safe and interoperable environment to use IoT devices and services. The purpose of this article is to answer the question that international standards can provide a safe and interoperable environment for IoT networks. The author determined the vulnerabilities and analysed the possible security solutions focusing on strengthens, weaknesses, opportunities, and threats. The results show specific issues with the use of IoT services, especially in a multinational environment.

Keywords: Internet of things, international standards, IoT vulnerabilities, IoT security

INTRODUCTION

Internet of Things (IoT) is one of the prominent and potential technologies which allows devices to be accessed from almost anywhere in the world. The first definition of IoT in the EU was presented by the Coordination and Support Action for Global RFID-related Activities and Standardisation (CASAGRAS) project in their final report in 2009, and it was defined as:

„A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor, and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity, and interoperability (CASAGRAS, 2009, p. 10)

The International Telecommunication Union (ITU) has defined IoT as „A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.“ (ITU-T, 2012, p. 1).

According to the above definitions, we can see that the IoT includes interconnected devices, which are able to provide information for the users via information and communication technologies (ICT). The main issue with the systems used IoT solutions is security, it is mandatory to use different cyber-security solutions in national and international environments. The author presents in this paper the security issues and possible solutions for national and international IoT solutions.

Research Questions:

- Is there any interoperable environment to use IoT systems in a multinational environment?
- Can international standards provide a safe environment for IoT devices and systems?

To answer these questions, the author collected the relevant literature using the Scopus and Google Scholar databases. Then the IoT standards, protocols, vulnerabilities were

determined. According to the results, the author finally analysed the possible security solutions using SWOT analyses.

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-20-5-NKE-5 New National Excellence Program of the Ministry of Innovation and Technology.

1 IOT STANDARDS AND PROTOCOLS

To understand the main issues with IoT usage in a multinational environment, firstly, it is needed to analyse the different standards and protocols of the devices, technologies, and communication solutions. There are claims about the need for common IoT standards, and there is an overwhelming number of standards for IoT, emanating from mainstream standards development organizations (SDOs), mainly from IETF[1], ITU-T, IEEE[2], ETSI[3], ISO/IEC[4], ISA[5], as well as other state-funded and international projects. They have plenty of different IoT solutions standards, including infrastructure, communication, transportation, security etc. According to these international guidelines, these organizations usually formulate international standards and requirements, and the national associations develop their own regulations. The main rule is that the national principles are always stricter than the international. It can use problem in multinational environments.

The organizations mentioned above develop the protocols for the different ICT solutions. In this case, it is the same as the IoT systems. The main protocols used in IoT services and solutions are the following:

- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) – a low power wireless mesh network where every node has its own IPv6 address;
- Bluetooth and Bluetooth Low Energy;
- Cellular (LTE/5G);
- CoAP (Constrained Application Protocol) – an internet productivity and utility protocol, is mainly developed for restricted smart gadgets;
- LoRaWAN (Long Ranged Wide Area Network) – a wide area network IoT protocol. LoRaWAN IoT Network Protocols is specifically designed to support the vast networks with the help of millions of low-power devices. Smart cities use this kind of protocol;
- MQTT (Message Queue Telemetry Transport) – it is a message and is mostly used for monitoring from a remote area in IoT. The principal task that MQTT does is obtaining data from so many electrical devices;
- RFID (Radio Frequency Identification) – a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to identify an object or person uniquely;
- X.509 – a standard for public key infrastructure (PKI) to manage digital certificates and public-key encryption. A key part of the Transport Layer Security protocol used to secure web and email communication.

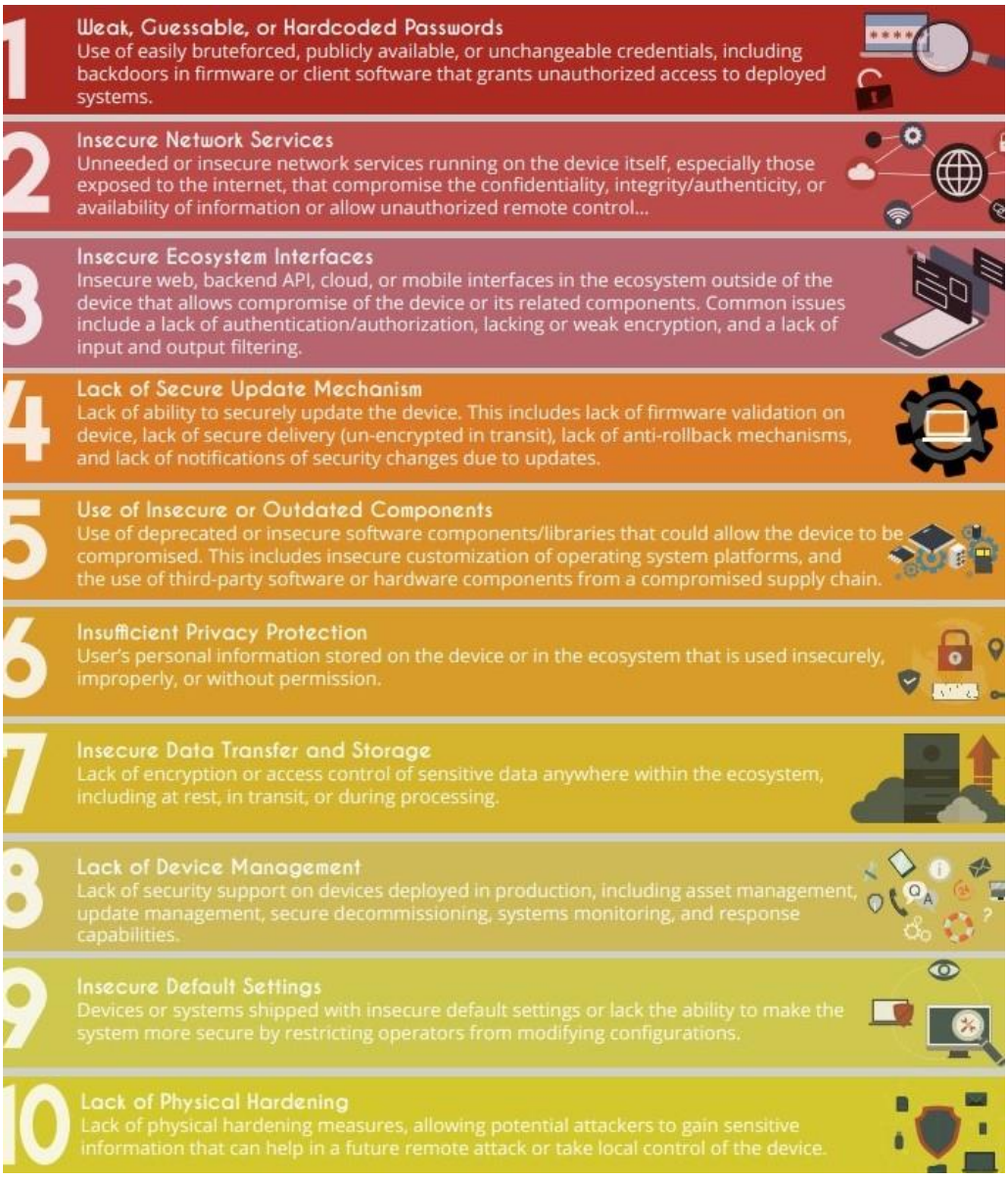
[1] IETF (Internet Engineering Task Force) – the leading Internet standards body. It develops open standards through open processes with one goal in mind: to make the Internet work better.
[2] IEEE (Institute of Electrical and Electronics Engineers) – a professional association that develops, defines, and reviews electronics and computer science standards.
[3] ETSI (European Telecommunications Standards Institute) – produces globally applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast, and internet technologies.
[4] ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission) – the ISO is an independent nongovernmental organization and the world's largest voluntary international standards developer. The IEC is the world's leading organization to prepare and publish international standards for electrical, electronic, and related technologies.
[5] ISA (International Society of Automation) – a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure.

- Wi-Fi;
- Zigbee – a wireless networking standard aimed at the remote control and sensor applications suitable for operation in harsh radio environments and isolated locations. (Yedle, Shrivastava, Kumar, Kumar, Kumar, 2020, p. 79-81)

These protocols and standards describe the various infrastructure, identification, transport, data, and security requirements. With them, it is possible to communicate in altered ICT environments used IoT solutions.

2 IOT VULNERABILITIES AND SOLUTIONS

According to the OWASP[6] IoT Team final report in 2018, the top 10 vulnerabilities in IoT systems and environments can be seen in Picture 1.



Picture 1 OWASP IoT Top 10
Source: OWASP IoT Top 10 Final Report

[6] Open Web Application Security Project

According to Picture 1, we can see that the most common issue with the IoT systems and devices is that weak, guessable passwords are used in the networks. The IoT devices come with pre-set, default credentials (usernames and passwords), which are often publicly available (can be found on the internet) and can be easily broken through brute-force attacks. With these weak password protections, the system can be exposed, for example, to social engineering attacks. It is possible to reduce potential vulnerabilities with strong password protection and two-factor authentication.

It is also expected that on the IoT devices insecure network services are running; in this case, sensitive information can be compromised, and authentication processes can be bypassed, and eavesdropping attacks can be executed. They can be avoided with lightweight cryptographic encryption techniques and secure internet connection usage.

In very many cases, IoT devices collect and store personal information, which can be compromised if hackers are able to bypass built-in security features and authentication protocols. The broader IoT system - including data stores and API interfaces - can also be leveraged to steal sensitive data unless properly secured. The lack of software integrity checks and unsecure software APIs can also cause malicious code injection with compromised authentication controls, weak encryption protocols, and non-optimized input/output filtering. With a chain of trust or API endpoint security (e.g., input-validation) solutions, it is possible to reduce these kinds of weaknesses.

To protect IoT systems and devices from being compromised, administrators and users must be able to send and receive real-time updates to all hosts as soon as possible. Without these updates and trusted forms of firmware validation, patch delivery, and security monitoring, IoT devices could run outdated versions with glaring code vulnerabilities, causing device software failures and unauthorized access.

Different other personnel risks may be present in the IoT environments. They can be insider threats (sabotage, fraudulent activities, corporate espionage), teamwork issues (issues in communication and/or coordination), and the use of illegal logical tools (hacktivism). They can be reduced with security awareness training and exercises. After them, the users can realize that the system errors are not the device's failure or system, but a possible attacker. It is also a big challenge that physical attacks can be executed against the IoT systems. They can be:

- theft of equipment, documents, backups;
- physical damage to equipment;
- modification of devices. (ENISA 2019, pp. 30-34)

Against these attacks, the best solutions would be the use of physical security clarifications like walls, fences, barbed wires, etc., but in many cases, it is not possible to use them, for instance, in smart cities, so it is challenging to avoid the physical attacks in the IoT environments.

3 SECURITY SOLUTIONS

The cybersecurity solutions can be divided into national and international parts. It is written above that standards and requirements are formulated in different legislation and doctrines at international level. They are valid for all nations, including the international environment. It means that European Union's legislation is legally binding for all EU members, but it is not mandatory to keep the regulation outside of the Union. If one IoT device is made somewhere out of the EU, the manufacturer is not obliged to build the security features and solutions into the equipment, which are formulated by the EU. The only exception is when the device is made directly for the EU market. If somebody or a company orders it from the internet

from a webpage located out of the EU, it is not guaranteed that the device will contain the EU standards.

, It is more difficult at the national level because the national legislation is always stricter than the international. It means that an international standard can be tightened at the national level. It is also specific at companies' level. An excellent example is an army for these specifications. The military devices use international and national standards, and they always have military standards and keep the equipment in the most secure environment.

The IoT devicescan be seen in Chapter 2 that the different vulnerabilities require different security solutions. The best IoT cybersecurity solutions are the followings:

- firewalls;
- antivirus / spyware / spam filters;
- application filtering;
- intrusion detection systems (IDS[7]), intrusion prevention systems (IPS[8]);
- demilitarized zone (DMZ[9]);
- virtual private network (VPN[10]);
- security policies;
- authentication;
- encryption;
- key management. (Alladi, Chamola, Sikdar, Choo, 2020)

Analysing the above security tools using in national and international environments, we can find advantages and disadvantages. To specify them, I used the SWOT analyses, to determine the internal and external helpful and harmful effects. I divided the above solutions into two parts. The first is the hardware and/or software-based physical and logical separation like using firewalls, routers for DMZs and VPNs, IPS and IDS, and filtering. The other part is the data security like encryption, key management, authentication, authorization. The internal origin analyses include the advantages and disadvantages of EU members' effects, the external includes the non-EU members'. The results of the analyses can be seen in Table 1 and Table 2.

[7] IDS (Intrusion Detection System) – a network security tool that analyses network traffic for malicious activity, vulnerability exploits, or policy violations that are attempting to infiltrate or steal data from a network.
[8] IPS (Intrusion Prevention System) is a network security tool that detects and blocks identified threats.
[9] DMZ (the demilitarized zone) – also known as a perimeter network or a screened subnetwork, is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks, usually from the public internet.
[10] VPN (Virtual Private Network) – a network solution that creates a safe, encrypted connection. Typically, it is used over a less secure network, such as the public internet. It uses tunnelling protocols to encrypt data at the sending end and decrypt it at the receiving end. The originating and receiving network addresses are also encrypted to provide better security for online activities.

Table 1 SWOT analysis of the physical and logical separation

SEPARATION SWOT ANALYSIS	HELPFUL	HARMFUL
INTERNAL ORIGIN	– national regulations are easy to enforce – the international and national classified systems can be separated from the internet – if one member is attacked the others' systems are safe – with VPN safe communication can be built among members or organisations – the IDS/IPS can increase the network security	– the national systems are separated from the international's – slow information-sharing – lot of different security policies – difficult information-sharing among members
EXTERNAL ORIGIN	– possibilities of using products from non-EU manufacturers – possibility of assigning non-EU states to an IoT device or system – IoT information-sharing via VPNs with non-EU members, they do not have access to the internal network	– easy to take advantage of the lack of update of the devices and systems – possibility of exploiting the lack of standards to attack – possible built-in backdoors to carry out attacks – one device is compromised the whole system is compromised

Source: made by the author

Table 2 SWOT analysis of the data security

DATA SECURITY SWOT ANALYSIS	HELPFUL	HARMFUL
INTERNAL ORIGIN	– national regulations are easy to enforce – the number of external attacks can be significantly reduced due to proper encryption – safe information-sharing – protected communication channels	– key sharing is difficult or impossible due to national regulations – national and international devices and systems do not communicate due to different encryptions
EXTERNAL ORIGIN	– external nations can access the IoT system with proper authentications – external nations can also access IoT devices with encryption tools and key sharing	– devices from non-EU manufacturers are not suitable for encryption – possible built-in backdoors to carry out attacks

Source: made by the author

In the above tables, we can see that to using IoT services in a multinational environment includes some difficulties. There are strengths, like reducing attacks due to encryption or

firewall solutions. We can separate the networks at different levels using DMZ and VPN. The weaknesses are that the national and international systems cannot communicate because of the different encryption, and information-sharing is also difficult because of the different security policies. The opportunities are the possibility to use devices from countries, which are not part of the international environment. It is also possible to connect external countries or organizations to the IoT systems with authentication or proper encryption. The threats are the lack of updates of the devices and firmware and the possibility that they do not use the required standards and are not suitable for encryption.

CONCLUSION

The IoT devices have become more widespread in domestic, national, and international use. For these services, as in any area of life, security is paramount. Various standards and regulations have been put in place at national and international levels to ensure security. They regulate the entire life cycle of devices from production to use. They are valid in the example inside the EU and at the members' level. The problem is when equipment comes from outside these environments, and in the case of IoT devices, they are most often manufactured in other countries.

It is necessary to provide a safe environment where data can be collect and store without any compromise. To reach it, different cybersecurity solutions must be used. However, these solutions may lead to different results at the national and international levels due to different regulations. There may be differences in encryption and authentication between established systems due to stricter national regulations, which may make it difficult to share information collected by IoT devices and systems. Backdoors and bugs can be installed into the devices by the manufacturers to be able to monitor the devices later.

To avoid this, the best solution would be to use domestic or federal IoT products. They use the necessary standards to build a safe environment, provide a secured network area to store, and share information. Unfortunately, this is not always possible, so devices are often used by manufacturers who are not reliable. In these cases, particular emphasis should be placed on the above protection solutions, which may be suitable in both international and national environments.

To answer the research questions, we can say that it is possible to build a safe and interoperable environment for IoT systems in multinational situations with the use of international standards. But next to this environment, there can be the national secured networks that are not compatible with it because of the national regulations and key management.

To summarise, it is possible to build safe and interoperable environments for the IoT services, but it is always needed the use of stricter national requirements because of the different manufacturers' devices and against the possible external attacks.

BIBLIOGRAPHY

ALLADI T., CHAMOLA V., SIKDAR B., CHOO K. R. Consumer IoT: Security vulnerability case studies and solutions. In *IEEE Consumer Electronics Magazine,* Volume: 9, 2020, Issue: 2, ISSN: 2162-2256, p. 17-25.

Coordination And Support Action for Global RFID-related Activities and Standardisation 2009. *Final report: RFID and the Inclusive Model for the Internet of Things,* [online]. Available on the internet:

https://docbox.etsi.org/zArchive/TISPAN/Open/IoT/low%20resolution/www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf

European Union Agency for Cybersecurity (ENISA) 2019. *Good practices for security of IoT*, Athen, 2019, p. 132, ISBN 978-92-9204-316-2

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) 2012. *Y.2060 Overview of the Internet of things*, [online]. Available on the internet: https://www.itu.int/rec/T-REC-Y.2060-201206-I

Open Web Application Security Project 2018. *IoT Top 10 Final Report*, [online]. Available on the internet: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

SHINDE G. R., DHOTRE P. S., MAHALLE P. N., DEY N. *Internet of Things integrated augmented reality*, Singapore, 2020. p. 89. ISBN 978-981-15-6373-7

YEDLE B., SHRIVASTAVA G., KUMAR A., KUMAR A. M., KUMAR T. M. A survey: security issues and challenges in Internet of Things. In *Advances in distributed computing and machine learning*. Singapore, 2020. ISBN 978-981-15-4217-6

Andras TOTH, PhD
Hungaria krt. 9-11, Budapest, H-1101, Hungary
toth.hir.andras@uni-nke.hu