# СТАТЬИ ПО МАТЕРИАЛАМ ПЛЕНАРНЫХ ДОКЛАДОВ
# ARTICLES BASED ON THE MATERIALS OF THE PLENARY REPORTS

UDC 004.056

## SECURITY ISSUES IN IoT DEVICES

V.A. Gasimov, G.A. Zahidova, A.A. Valiyeva, L.R. Zeynalli-Huseynzada
*Baku Engineering University, Baku, Azerbaijan*

**Abstract.** Although the widespread use of Internet of Things (IoT) technologies increases the efficiency of information systems, the limited computing capabilities and weak security mechanisms of IoT devices make them vulnerable to various cyberattacks. This thesis analyzes the main security problems occurring in IoT devices, a real cyber incident example, and effective protection methods. As a result, it is determined that IoT security requires a complex and multi-level approach.
**Keywords:** IoT; cybersecurity; authentication; encryption; botnet; DDoS; firmware; network security; security risk; defense mechanism.

### Introduction

The Internet of Things (IoT) is a technology that enables physical objects, sensors, and various smart devices to communicate with each other via the Internet and exchange information. The IoT system has the ability to collect, process, and transmit information in real time. This technology creates integration between the physical environment and digital systems, making management processes more efficient and automated. The application areas of IoT are quite wide. Remote monitoring of patients in the healthcare sector, automation of production processes in industry, intelligent management systems in transportation, productivity monitoring in agriculture, and smart home systems are some of the main areas where IoT is widely used. This technology not only increases economic efficiency, but also expands operational decision-making capabilities.

According to reports from international organizations such as Cisco Systems and Gartner, billions of IoT devices are in use worldwide and are increasing every year. However, the widespread use of IoT devices has also raised security concerns. Poor protection of these devices can lead to cyberattacks, data leaks, and even disruption of critical infrastructure. Therefore, investigating security issues in IoT devices is of great scientific and practical importance.

### Primary Security Issues

The widespread adoption of the Internet of Things ecosystem and its application in various fields have made security issues even more critical. Unlike other information systems, IoT devices are characterized by a lack of computing power, poor memory resources, as well as energy constraints.

In addition, IoT devices are used in an open network environment, but they are not configured with the required security features. This has made IoT systems easy targets for cyber attackers.

The concerns in IoT security include both technical and organizational issues. It involves the protection of information systems in a manner that ensures the integrity, availability, and confidentiality of the information are not compromised in the hands of unauthorized persons. However, the risks are not limited to the devices alone but also the infrastructure that houses the devices.

The primary security issues associated with IoT devices are as follows.

*1. Inadequate Authentication and Authorization Mechanisms.* Perhaps one of the most common security issues when it comes to IoT devices starts right at the very beginning, as many devices are preconfigured with a default username/password combination. In many cases, the end user never bothers changing this combination. As a result, attackers have it very easy when it comes to launching a brute force attack. And then, of course, there is the role-based access control, which is not very well implemented in many cases, allowing attackers to gain access to many more rights than they should ever need. For example, someone who should only have 'read-only' rights could end up being granted the master key. And if the authentication process is not robust enough, then the threat of botnet attacks looms very large.

*2. Encryption and data protection issues.* Data security in IoT devices raises two important issues: Data in Transit, Data at Rest.

Data in Transit: In many IoT systems, data is sent over unencrypted channels, e.g., HTTP. This leaves the system open to a "Man-in-the-Middle" attack, where the hacker gains access to the network, allowing him to observe, modify, or even forge the data stream.

Data at Rest: Inadequate handling of cryptographic algorithms, improper handling of certificates, lack of proper handling of keys within the device, as well as hard-coding keys into the application, are some of the issues related to data at rest.

*3. Lack of firmware and software updates.* The lifespan of IoT devices is quite long (up to 5–10 years). This leads to the problem of outdated software. The fact that updates in the firmware are:

– not done in an automated way;

– not transmitted in an encrypted way;

– not supported at all.

They make it possible for the system to be in use for a long time with known vulnerabilities. Moreover, the update mechanism in this case can be a threat because the update package is not protected by a digital signature. This makes it possible for the attacker to download fake firmware.

*4. Network architecture weakness and segmentation issues.* IoT devices are deployed in close proximity to other critical systems in the same network. The absence of network segmentation allows an attacker to use a compromised IoT device to access other systems in the network, thereby enabling lateral movement. This issue represents a significant threat, particularly in industrial IoT environments, which may result in stopping production in these environments.

*5. Botnet and DDoS attacks.* The high number of IoT device infections by malware results in botnet attacks. For instance, in 2016, the Mirai botnet attack caused a DDoS attack on Dyn, which temporarily restricted access to online platforms such as Twitter, Netflix, and GitHub. Therefore, IoT security affects the global internet infrastructure.

*6. Privacy and data abuse.* IoT devices collect different kinds of data about their users' daily lives, such as: geolocation data, biometrics, indoor activity data, voice commands, etc.

The lack of proper security for this data poses a significant threat to user privacy. Moreover, data transfer to third parties or use for commercial purposes may lead to ethical and legal issues. As a result of data leakage, users may be at risk of suffering different kinds of attacks, such as financial loss, identity theft, or blackmail.

*7. Physical intrusion and hardware-level attacks.* In most cases, IoT devices are installed in an uncluttered area (production area, public area, etc.). Once the attacker is able to gain physical access to the device, he can:

Access the firmware through the JTAG and UART interfaces,

Obtain the cryptographic keys from the memory,

Re-program the device.

The threat of such types of attacks is critical, especially in the industrial and transportation sectors.

*8. Lack of standardization and regulation.* The IoT environment has developed without a set of standard security rules; therefore, manufacturers have a patchwork of security standards. There are some who are taking security in the IoT seriously, but some are compromising to be competitive and save money. In this case, the combination of different security standards in a network compromises the entire network.

However, IoT security is not only a technical issue but also has significant social, economic, and strategic ramifications. Today, IoT devices are involved in various aspects of life, such as smart homes and industries, healthcare, and services. The security concerns associated with IoT are not only significant for the systems but also for the overall society and people in various ways.

The level of concern regarding IoT security is substantial. IoT devices have the ability to accumulate an enormous volume of data from our daily lives. These include location information, audio, video, health information, and much

more. Because of these issues, it is entirely possible for an individual to intercept data being collected by IoT devices. In doing so, it creates an opportunity for various types of cyber crimes such as identity theft, financial crimes, privacy invasion, blackmail, and much more. A good example is an intelligent security camera and an intelligent home management system. Intercepting data from such devices is an invasion of one's personal space.

In the case of the corporate world, IoT security risks can cause more economic losses. Industrial IoT networks are connected to manufacturing, logistics, and energy management systems. An IoT cyber-attack can cause losses in the form of downtime and data losses. In 2016, the DDoS attack performed by the Mirai botnet on Dyn's services caused a shutdown of Twitter, Netflix, and GitHub services for a few hours. This is an example of how IoT security risks can cause damage to the global economic system.

In the case of the national and critical infrastructure world, the risks are more critical and can cause more damage to the system as a whole. Energy management systems, transportation systems, healthcare services, and government services are using IoT technology. In such cases, the damage caused by IoT security risks can cause more harm to the system and can even cause a threat to human life, as in the case of information loss.

In addition, security issues in IoT devices can lead to legal and ethical risks. Non-compliance with data protection legislation can result in a heavy financial penalty for companies. In addition, the unregulated collection and processing of users' information can result in a lack of public trust in companies, thereby slowing down the digital revolution.

In conclusion, the scope of security issues in IoT devices can be from individual users up to global infrastructure levels. The risks can be managed through various means: technology, legislation, standardization, and security by design. Therefore, IoT security can be viewed as a strategic issue in the information society.

## Conclusion

From the analysis above, it is obvious that security issues related to IoT devices are systemic and complex. In other words, the lack of proper authentication and authorization processes, encryption issues, the absence of firmware updates, poor segmentation of the network, botnet and DDoS attacks, privacy issues, physical intrusion capability, and the lack of proper standardizations represent the main security issues of the IoT environment.

The limited availability and regulation of resources in this environment make information devices more vulnerable to criminal attacks compared to other information systems. This is not just a threat to an individual; rather, it is a problem that needs to be addressed by an organization. One good example is the Dyn DDoS attack in 2016, which was executed by a botnet called Mirai. This

attack also proves the significance of the role played by IoT in determining the worldwide internet landscape.

Based on the results obtained, it has been concluded that the security of IoT devices is not ensured only through technical means of protection. The following complex approach is crucial for the security of IoT devices.

1. The implementation of reliable methods of authentication and multi-factor authentication.

2. The application of modern methods of cryptography during data transmission and storage.

3. The application of reliable and digitally signed methods of firmware update.

4. The application of the "zero trust" approach and the segmentation of the IoT network.

5. The application of the "security by design" approach, taking into account the security issues from the design phase.

6. The improvement of international standards and mechanisms.

Therefore, it may be stated that the security aspect in the context of IoT not only involves a technical challenge but also has a number of strategic, economic, and social implications. Thus, it may be stated that in the context of a secure and sustainable growth of the IoT technology, it is not only a matter of choice but a matter of necessity for the government, industry, and the end-users to come together in order to unlock the true potential of the technology.

## References

1. Weber R.H. (2010). *Internet of Things – New security and privacy challenges.* Computer Law & Security Review, 26(1), 23–30.

2. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. (2015). *Security, privacy and trust in Internet of Things: The road ahead.* Computer Networks, 76, 146–164.

3. Atzori, L., Iera, A., & Morabito, G. (2010). *The Internet of Things: A survey.* Computer Networks, 54(15), 2787–2805.

4. Roman R., Zhou J., Lopez J. (2013). *On the features and challenges of security and privacy in distributed Internet of Things.* Computer Networks, 57(10), 2266–2279.

5. Stallings W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards.* Addison-Wesley.

6. Conti M., Dehghantanha A., Franke K., Watson S. (2018). *Internet of Things security and forensics: Challenges and opportunities.* Future Generation Computer Systems, 78, 544–546.

7. Granjal J., Monteiro E., Silva J.S. (2015). *Security for the Internet of Things: A survey of existing protocols and open research issues.* IEEE Communications Surveys & Tutorials.

## Information about the authors

**Gasimov V.A.,** Professor, Dean of the Faculty of Information and Computer Technologies, Baku Engineering University, vaqasimov@beu.edu.az.

**Zahidova G.A.,** Lecturer of Cybersecurity and Computer Engineering Department, Baku Engineering University, guabdullayeva@beu.edu.az.

**Zeynalli-Huseynzada L.R.,** Lecturer of Cybersecurity and Computer Engineering Department, Baku Engineering University, lzeynalli@beu.edu.az.

**Valiyeva A.A.,** Assistant of Cybersecurity and Computer Engineering Department, Baku Engineering University, aveliyeva@beu.edu.az.