УДК 004.056

Вакуліч В.І.
Магас Л.М.

VULNERABILITY ANALYSIS OF THE INTERNET OF THINGS (IOT)

Vinnytsia National Technical University

Abstract
This work reviews the literature to better understand privacy and security issues in IoT devices and how people understand them. The responses were grouped into categories to recognize data on different topics.

Keywords**:** *Internet, Internet of Things (IoT), security and privacy, devices, quality.*

Анотація
В даній роботі зроблено огляд літератури, щоб краще зрозуміти питання конфіденційності та безпеки в пристроях Інтернет речей та їх розуміння людьми. Відповіді були згруповані за категоріями для розпізнавання даних за різною тематикою.

Ключові слова**:** *Інтернет, Інтернет речей (IoT), безпека та конфіденційність, пристрої, якість.*

Introduction

Today, the Internet of Things (IoT) is not just a vision or research topic, it is already becoming reality. Examples of IoT systems include smart homes with smart door locks, garden mowers, or smart fridges; smart cities where sensor networks measure air quality or display free parking spots; and companies and organizations where smart buildings manage energy and heating or CCTV cameras monitor premises. According to Siemens[2], the number of IoT devices worldwide is estimated to reach 75.4 billion by 2025 [1].

Basics

The Internet of Things is a multi-layered architecture, with each layer having its own set of functions and using different technologies to perform those functions. The rapid proliferation of IoT devices raises various types of security concerns. For example, authentication, authorization, confidentiality, integrity, and privacy are all potential threats. These threats lurk at different levels of the IoT architecture and need to be addressed accordingly [2].

The hardware of an IoT device is usually composed of the sensor, actuator, and built-in communication module (Gubbi, Buyya, Marusic, & Palaniswami). IoT devices use two connection modes to collect sensor data from monitored targets. One is a wireless connection, such as ZigBee, Bluetooth, orwi-fi, and another mode is wired connection, such as Ethernet, Hahm, Baccelli, Petersen, and Tsiftes classified IoT devices into 2 categories based on their operating system (OS): high - end IoT devices and low-end IoT devices. High-end IoT devices can run traditional OS such as Microsoft, or Linux. Low-end IoT devices can only run lightweight or customised OS. The performance of IoT devices normally depends on energy capacity, memory, and CPU. The physical size of the IoT device is generally small. Its memory and CPU performance lags far behind other common computersand laptops and it is not practical to run complex software and perform complex computations.

The most common attacks on IoT:

DDoS attack: occurs when a botnet - an infected network of computers - continuously sends a huge number of requests to the system. Abnormally high activity can lead to significant delays in the system's operation or even to its shutdown. A well-adjusted and customized DDoS attack can cause a system error of a security component, hiding the real malicious actions. Moreover, infected IoT devices can also become part of a botnet and help attackers conduct even more destructive attacks from inside the local network, which usually has a higher level of trust in information security systems.

Software exploit: Many cybercriminals use already known vulnerabilities in the software part of a device to conduct an attack. Developers usually close the security holes they find in updates. However, it is not always the case that the latest software versions are downloaded to devices in time. This makes them vulnerable to exploit attacks.

MITM (man-in-the-middle) attack: Hackers can intercept network traffic (by standing in the middle of the transmission channel between the sending device and the receiving device) and obtain credentials or sensitive information that IoT devices transmit through corporate networks. Since many smart devices are usually not even encrypted, it will be very easy for an attacker to use the data obtained to gain unauthorized access to the system.

Physical interference: a cybercriminal simply plugging a USB flash drive with malicious code into an external IoT device can be enough to spread malware across the network and spy on communications.

Brute-force attacks: The fact that companies typically do not pay enough attention to password security for IoT devices leaves them vulnerable to potential brute-force or "brute-force" attacks. Often, the passwords of IoT devices remain unchanged after installation by simply using a basic password, which makes it very easy for attackers to pick them.

Firmware hijacking: If a device's firmware update is not cryptographically signed or if the firmware is transmitted over an insecure communication channel, it allows attackers to intercept it and download malware to devices under the guise of updates. The stolen firmware also gives cybercriminals the opportunity to obtain device credentials. Using the credentials, they can gain access to corporate networks or other systems that store confidential information. Thus, an attack on a seemingly innocent device can turn into a full-blown data breach [3].

From the above attack vectors on IoT, it can be concluded that the main components of IoT systems are quite vulnerable to attack by intruders. Regardless of the scale and type of environment in which an IoT system is being embedded, security should be considered at the design stage to improve its integration. A particular challenge for engineers and information security officers is that, due to the technological features of IoT, installing an agent to check for infections or vulnerabilities is not allowed.

To protect IoT devices, you should follow the following rules:

Manage the attack surface, inventory, and monitor all devices: When planning for IoT security, one of the main tasks should be to create a map of connected devices for inventory purposes. Security teams need to know the exact number of devices in use, as well as manufacturer IDs, serial numbers, hardware versions, and firmware.

Network segmentation: In the event of a successful cyberattack, an attacker can gain access to an organization's entire network. Segmentation prevents this by limiting the attack surface and minimizing damage. Network segmentation is the process of dividing an internal network into several separate subnets.

Setting strong passwords for IoT: Many IoT devices come with weak pre-set passwords that are very easy to pick. As soon as an IoT device first registers on your network, the best practice is to change its preset password to a much stronger one.

Secure all IoT devices at the physical level: Physical protection of devices is very important, as devices that are accessible from the outside can be physically tampered with by attackers to gain unauthorized access or download malware to the system. Therefore, you should ensure that the device is located in a secure location so that it is not openly accessible.

Timely firmware updates: Newer firmware versions may have fixes for existing software vulnerabilities in the device. That's why keeping them up-to-date on a regular basis will go a long way toward improving overall IT security [4].

Following the above recommendations will help people to use IoT devices safely, taking full advantage of their benefits while minimizing the risks they can pose. But keep in mind that cyberattacks are constantly evolving and becoming more sophisticated.

Conclusion

In conclusion, the Internet of Things (IoT) presents a multi-layered architecture with its own set of functions and technologies, but its rapid proliferation also brings forth significant security concerns. Authentication, authorization, confidentiality, integrity, and privacy are all potential threats that exist at various levels of the IoT architecture and require appropriate attention. The hardware components of IoT devices, including sensors, actuators, and communication modules, play a crucial role in IoT systems. Common attacks on IoT, such as DDoS attacks, software exploits, MITM attacks, physical interference, brute-force attacks, and firmware hijacking, highlight the vulnerabilities of IoT systems. To protect IoT devices, it is essential to prioritize

security at the design stage, manage the attack surface, implement network segmentation, set strong passwords, ensure physical protection, and regularly update firmware versions. These measures contribute to enhancing the overall security and reliability of IoT systems in today's interconnected world.

REFERENCES

1. With the Internet of Things set to near URL: https://www.zerocarbonacademy.com/posts/with-the-internet-of-things-set-to-near-30-billion-devices-by-2025-tech-giants-are-facing-pressure-to-address-the-growing-environmental-impact-their-products-pose
2 Vulnerability Management for Internet of Things (IoT) Security URL: https://blog.rsisecurity.com/vulnerability-management-for-internet-of-things-iot-security/.
3. Поширені атаки на IoT URL: https://corewin.ua/blog/attacks-on-iot-how-protect/.
4. Vulnerability association evaluation of Internet of thing devices based on attack graph URL: https://journals.sagepub.com/doi/full/10.1177/15501329221097817.

Liudmyla M. Magas – Lecturer of English, FL department of Vinnytsia National Technical University, Vinnytsia.

Vakulich Vadym Ihorovych – student of group УБ-21б, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: vakulicvadim61@gmail.com

Магас Людмила Миколаївна – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця.

Вакуліч Вадим Ігорович – студент групи УБ-21б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: vakulicvadim61@gmail.com