СЕКЦІЯ 5
КІБЕРБЕЗПЕКА І ЗАХИСТ ІНФОРМАЦІЇ

UDC 004.738:004.77

CYBERSECURITY IN THE INTERNET OF THINGS (IOT): CHALLENGES AND PROTECTION STRATEGIES

Drakon D.S., student, daria.drakon@student.karazin.ua, ERI "Karazin Banking Institute" V.N. Karazin Kharkiv National University
Stiahlyk N.I., Ph.D., Head of the Department of Information Technology and Mathematical Modelling "Karazin Banking Institute", natalia.stiahlyk@karazin.ua, V.N. Karazin Kharkiv National University

In today's world, where internet-connected devices are becoming an integral part of our everyday lives, cybersecurity in the Internet of Things (IoT) realm is becoming increasingly pertinent. In the context of the increasing number of devices connected to the internet, cybersecurity in the Internet of Things (IoT) domain is becoming increasingly pertinent. It involves the development and implementation of strategies and security measures to protect IoT devices from cyberattacks, unauthorized access, and data breaches. However, before delving into discussions about challenges and protection strategies, let's understand what the Internet of Things entails and how it impacts our lives.

Technical definition: The Internet of Things (IoT) is a network of interacting devices, including sensors, actuators, and other devices, equipped with electronics, software, and network connections that enable them to collect and exchange data.

In the simple words The Internet of Things (IoT) refers to the connection of ordinary objects to the internet, enabling them to become smart and capable of exchanging data with each other and with us [1].

Attacks on IoT infrastructure are becoming increasingly prevalent, with attackers exploiting these devices to orchestrate large-scale attacks while remaining undetected. This highlights the critical importance of implementing robust security measures to safeguard IoT ecosystems from potential threats.

Image 1 - Microsoft statistic of attack to IoT devices [2]

In one of theirs articles, Microsoft provided statistics indicating the number of users who have been subjected to cyber-attacks on their IoT devices (Image 1). It is evident from the data that over half of the users have experienced or have been targeted by attempted cyber-attacks at least once.

All of this, of course, could be seen as a marketing campaign, as the statistics were provided by Microsoft for their new security program, but unfortunately, the threat is real. In recent years, Ukraine has been subjected to at least five attacks, and these were the most ambitious and well-known. Here are some examples: TeleBots attacks on financial institutions (2016), NotPetya attack (2017), hacker attacks on Ukraine in June 2017, which paralyzed the networks of “Boryspil” airport, “Ukrposhta”, “Ukrzaliznytsia”, the website of the Cabinet of Ministers and a number of other enterprises, hacking of smart cameras (2019). And since February 24, 2022, the threats of attacks in Ukraine have only intensified.

Taking into account all of the aforementioned, the following challenges [3] confronting IoT can be delineated:

— **Limited computational and storage resources**: Many IoT devices suffer from limited computational and storage resources, reducing their ability to implement modern security measures and increasing their vulnerability to attacks.

— **Insufficiently secure boot process**: Devices are at risk of attacks during their boot process, which elevates their level of vulnerability.

— **Open communication ports**: The presence of open communication ports creates a vulnerability that malicious actors can exploit to gain access to devices, especially in open network conditions.

— **Insufficient encryption and authentication/authorization**: Insufficient data encryption measures and weak authentication and authorization mechanisms leave the information on devices vulnerable to leaks and unauthorized access.

— **Design and development deficiencies**: Insufficient attention to security aspects in the design and development process of IoT devices can lead to vulnerabilities in them.

— **Deficiencies in updates and support**: The absence of regular updates and insufficient support from manufacturers make devices vulnerable to new threats.

— **Insufficient skills in the field of IoT and lack of security standards**: The lack of qualified specialists and the absence of unified security standards hinder the development and application of effective protective measures.

— **Data privacy issues**: Insufficient data protection increases the risk of confidential information leaks and privacy breaches.

— **Physical security threats**: Physical attacks, such as theft or damage to devices, pose a serious threat, especially in critical infrastructure or medical devices.

— **Issues with various interfaces (web, mobile, cloud):** Vulnerabilities in various interfaces can be exploited by malicious actors to attack devices and their data.

Enhancing IoT systems and combating attacks in the modern world is a key task. The strategies themselves are directly derived from the challenges. The following strategies can help improve the IoT security system. Here's how the proposed strategies can be linked with the proposed methods to address the challenges in IoT security:

— **Encryption and Strong Authentication**: The implementation of robust data encryption methods and strong authentication mechanisms contributes to the protection of information confidentiality and integrity during its transmission and storage.

— **Regular Testing and Updates**: Conducting thorough security testing and regular updates of IoT devices are important measures for detecting and rectifying vulnerabilities, enhancing the overall resilience of the system.

— **Password Care:** Educating users about the significance of setting reliable, unique passwords for IoT devices helps prevent brute-force password attacks and protect devices from compromise.

— **Best Practices in IoT Security:** Promoting the use of industry best practices in IoT security, such as secure programming, vulnerability management, and adherence to recognised security standards, contributes to enhancing device security levels.

— **Network Security Measures:** Deploying robust network security measures, including firewalls and intrusion detection systems, helps protect devices from network attacks, such as Denial of Service (DoS) attacks.

— **Standardisation Efforts:** Advocating for IoT security standards and protocols contributes to achieving consistency and compatibility among devices and systems, ensuring secure development practices.

— **Privacy by Design:** Priority is given to privacy by design principles for protecting user data. Transparency regarding data collection and use, and respect for rights to control information, help maintain privacy.

— **Firmware and Software Updates:** Timely release of patches and security updates for IoT devices allows for the mitigation of software vulnerabilities and potential threats.

— **Employee Training:** Training employees and contractors about IoT security risks and awareness of threats from internal users are key factors in forming a security-oriented culture.

Conclusion. In the modern world, internet-connected devices are becoming an integral part of everyday life, giving cybersecurity in the field of Internet of Things (IoT) an increasingly significant character. The growth in the number of network-connected devices underscores the critical importance of developing and applying security strategies to protect IoT devices from cyberattacks, unauthorised access, and data leaks.

However, despite all the advantages that IoT brings, there are certain challenges, including limited computational and storage resources, insufficiently secure boot process, open communication ports, insufficient encryption and authentication/authorisation, as well as problems in design and development, support and updates, lack of qualified specialists and security standards, data confidentiality, and physical threats.

Improving the security of IoT systems and combating attacks is a paramount task in the modern world. The adopted strategies directly stem from these challenges, including encryption, regular testing and updates, password protection, adherence to best practices in IoT security, standardisation, and staff training. Such a comprehensive approach is necessary to ensure the security of IoT devices and the confidentiality of user data.

References

1. Microsoft Azure. What is IoT? [Internet]. Microsoft Azure, Dictionary. Available from: https://azure.microsoft.com/pl-pl/resources/cloud-computing-dictionary/what-is-iot. Accessed: 15 February 2024.

2. Microsoft. IoT Security Solutions [Internet]. Microsoft. Available from: https://www.microsoft.com/pl-pl/security/business/solutions/iot-security. Accessed: 17 February 2024.

3. Thales. Top IoT security issues and challenges (2022) [Internet]. Thales Group. Available from: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats. Accessed: 21 February 2024.

4. IoT Security: Strategies, Challenges, and Essential Tools [Internet]. DZone. Available from: https://dzone.com/articles/iot-security-strategies-challenges-and-essential-t. Accessed: 21 February 2024.