УДК 004.67

А.М. Медяна

INTERNET OF THINGS SECURITY

Vinnytsia National Technical University

Анотація

Стаття досліджує вплив Інтернету речей (IoT) на сучасне суспільство та визначає ключові виклики, пов'язані з його безпекою. Зокрема, розглядаються технології, що забезпечують функціонування IoT, виокремлюються чотири причини, чому безпека Інтернету речей повинна бути обов'язковою для всіх пристроїв. Автори також наголошують на необхідності заходів для забезпечення надійного захисту даних та пристроїв у світі швидкого розвитку IoT.

Ключові слова: Інтернет речей, безпека, технології, зв’язані пристрої, виклики, захист даних, стандарти безпеки.

Abstract

This report is dedicated to the use of machine learning methods in the field of threat analysis and risk management. It examines current technological approaches and algorithms that can effectively identify potential threats and improve decision-making processes in the context of risk management.

Keywords: Internet of Things (IoT), technology, security, communication, data protection, connectivity, cloud computing, machine learning, artificial intelligence, device security, regulatory compliance, privacy, cyber threats.

Introduction

The Internet of Things (IoT) is a modern phenomenon that is changing the way we communicate with technology and interact with the world around us. Thanks to the IoT, objects that used to be just "things" without an Internet connection now support the ability to share data and support actions that make our ubiquitous lives easier and better.

The protests, along with the undoubted benefits that IoT brings, also raise serious questions about the security of this new technology. The essence of IoT is to prevent billions of devices from connecting to the Internet, which collect, process, and share vast amounts of data. But with each new connected device, the probability of a cyber threat increases, which can threaten both our privacy and security in general.

The purpose of our research is to get a deeper understanding of Internet security and identify some threats, understand how they affect our lives, and propose effective measures to prevent them. Knowing about IoT security allows us to get the benefits of this technology while maintaining our privacy, protecting data and providing robust protection against some threats.

Research results

The term Internet of Things (IoT) was first coined by the British entrepreneur Kevin Ashton back in 1999. With this term, he described the concept of an international network of RFID devices. Today, IoT contains applications in various areas of our life - in projects of safe cities and intelligent buildings. What does all this mean for market safety? Companies from the Security 50 list of the most successful manufacturers of security solutions have shared their opinion with us.

To begin with, it is worth noting that physical security is inextricably linked to IoT. This is especially evident when you consider that the security industry is moving massively to IP technologies that allow the device to be integrated into the Internet environment. "Security products are part of the IoT," said Allen Liu, product manager of Dahua Technology. "Video surveillance, mobile devices, access control systems, security systems - all this equipment, which we are separated in our ubiquitous life, can be connected to each other with the help of the Internet."

The integration of various devices for working on the Internet provides many advantages. They include increased security, better intelligence and convenience for users [1].

The Internet of Things (IoT) helps people live and work smarter, and puts them in full control of their lives. In addition to offering smart devices for home automation, IoT is an integral part of business. IoT enables businesses to gain a real-time view of how their systems are actually performing, providing insight into everything from machine performance to supply chain and logistics.

IoT allows companies to automate processes and reduce labor costs. It also helps to reduce wastage and improve service delivery by making the manufacture and supply of goods less expensive and providing transparency in customer transactions.

IoT is one of the most important technologies in everyday life, and it will continue to gain momentum as more enterprises understand the potential of connected devices to ensure their competitiveness [2].

With the help of affordable computing systems, cloud technologies, big data, analytics and mobile technologies, physical objects can exchange and collect data with minimal human intervention. In this hyper-connected world, digital systems can record, monitor and configure every interaction between connected things. The physical world meets the digital world and they collaborate [3].

Although the idea of the Internet of Things has been around for a long time, recent advances in a number of different technologies have made it practical. Namely:

- access to inexpensive sensors with low energy consumption. Affordable and reliable sensors allow larger manufacturers to use Internet of Things technology;
- connectivity. A large number of network protocols for the Internet facilitate the connection of sensors to the cloud and other "things" for efficient data transmission;
- cloud computing platforms. The increasing availability of cloud platforms allows both businesses and consumers to access the infrastructure they need to scale without having to manage it;
- machine learning and analytics. With advances in machine learning and analytics, and access to diverse and large amounts of data stored in the cloud, businesses can gain insights faster and easier. Advances in these related technologies continue to expand the capabilities of the Internet of Things, and the data generated by the Internet of Things also fuels these technologies;
- conversational artificial intelligence (AI). Advances in neural networks have led to the introduction of Natural Language Processing (NLP) in IoT devices (e.g, digital personal assistants Alexa, Cortana, and Siri), making them attractive, accessible, and suitable for home use [3].

Four reasons why internet of things security should be mandatory for all devices

1. The IoT now consists of billions of devices that can be connected to each other. And while you might think that the chances of someone finding your device are statistically unlikely, you'd be dead wrong. Simply connect a Linux machine to the Internet with the default administrator password and watch how quickly that device is discovered and hacked.

2. Customers need the integrity of their personal data to remain private and secure. Companies are developing apps that collect and store data on sleep patterns, heart rate, nutrition, exercise, travel, and countless other data. It is extremely important to users that their data is not used, shared publicly or used in any other way without their express consent. In today's world, we all know how valuable data is, and if you can't protect that data, customers will go somewhere else that they believe will protect it. In addition, the legislation requires the protection of personal data.

3. A compromised device or its data can lead to huge potential losses for both the customer and the device manufacturer. Developing and launching a product is expensive and often involves the development of numerous intellectual property objects such as source code. A device security breach can expose years of software development. This would allow hackers to use the software for their own purposes or sell trade secrets to competitors.

4. IoT security is no longer optional as world governments step in and start regulating the Internet. Take for example the fine just issued by Facebook. Hackers want to gain access to an IoT device and use its data in some way, and governments are starting to target tech companies that don't take security seriously. There are several examples of new regulations such as the European General Data Protection Regulation (GDPR), the IoT Cybersecurity Improvement Act of 2019, and California SB-327 [4].

Many manufacturers consider protecting their product a nice-to-use feature rather than a must-have. The thought of someone trying to attack, hack, or exploit their product seems far-fetched and unimportant, improbable and difficult. Companies are often focused on getting their product to market with the features they need to support their customers. At the same time, security is simply not considered a priority in today's rapid product development cycle.

However, today IoT security for any connected device has become an important and basic requirement.

Let's take for example several events in the recent past involving security breaches of connected devices. The first, and probably the most famous among developers of embedded programs, were hackers. They were the ones who found a way to remotely access Jeeps and control various settings while the car was moving! Hackers were even able to control systems such as the engine, power steering and brakes. This is one of many examples that shows that the security of the Internet of Things should be at the top of the requirements when designing devices.

Another example was the recent recall of nearly 500,000 pacemakers due to holes in the firmware that allowed remote hackers to gain access and control the pacemaker. In fact, security is overlooked and underestimated so often. For example, a group of hackers recently created a killer program that could

control an insulin pump because the manufacturer did not take their reports of security vulnerabilities seriously [4].

Conclusion

In the conclusion to the essay on the security of the Internet of Things (IoT), it can be emphasized that the growth of IoT in our modern world inevitably brings with it new challenges and threats in the field of security. While IoT offers many benefits and opportunities for organizations, it also faces significant risks associated with the increased volume of connected devices and the exchange of large volumes of data.

IoT security concerns include the potential for hacking by attackers, leakage of personal data, insecure information sharing, and risk to critical infrastructure. Insufficient IoT security can lead to serious consequences, such as leakage of confidential information, violation of user privacy and destabilization of critical systems.

However, given these risks, steps can be taken to ensure IoT security. This includes improving device security, establishing data protection, developing security standards, and collaborating among manufacturers, users, and organizations to identify and eliminate potential threats.

The next steps in the development of the security of the Internet of Things should be aimed at ensuring reliable protection of devices and networks, developing security standards and increasing security awareness among users and professionals. Only through joint efforts can we create a reliable and secure environment for the development of the Internet of Things, which will benefit both organizations and users.

REFERENCES

1. Безпека та Інтернет речей – пов'язані разом. URL:https://worldvision.com.ua/articles/bezopasnost-i-internet-veshchey-svyazani-vmeste
2. What is the internet of things (IoT)? URL: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT
3. What is IoT? URL: https://www.oracle.com/internet-of-things/what-is-iot/
4. Безпека інтернету речей. URL: https://oxorona.com/iot-security/

Медяна Аліна Миколаївна – студентка групи УБ-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: medanaa904@gmail.com

Науковий керівник: ***Андрощук Катерина Миколаївна*** — викладач кафедри іноземних мов, Вінницький національний технічний університет, м. Вінниця

Alina Medyana M. – *student of UB-22b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: medanaa904@gmail.com*

Supervisor: ***Androshchuk Kateryna M.*** – Lecture, Chair of Foreign Languages, Vinnytsia National Technical University, Vinnytsia.