SUMMARY ACCORDING SECURITY THREATS TO THE INTERNET OF THINGS

Norkuvvat Chunaev
Tashkent University of Information Technologies named after Muhammad Al-Xorazmiy,
Jakhongirbek Khabibullaev
Tashkent University of Information Technologies named after Muhammad Al-Xorazmiy,

Abstract: *The concept of the Internet of Things (IoT) was introduced by Kevin Ashton at MIT in 1998. The vision of the concept is that objects, "things", are connected to each other and therefore create an IoT in which each object has its own individual identity and can interact with other objects. Internet of Things objects can vary greatly in size from small to the largest. The Internet of Things turns ordinary products such as cars, buildings and machines into smart devices, connected objects that can communicate with people, applications and each other. In the paper, we examine the prevalence of the Internet of Things in today's world and its impact on various industries. The paper discusses the security threat of the Internet of Things and as a result, security recommendations will be made.*

Keywords: *Internet of Things, NB-IoT, cybersecurity, security threats, computer security.*

Devices connected to the Internet of Things (IoT) have become an integral part of everyday life. The Internet of Things is growing rapidly as more and more devices connect to the global network. The data and applications of many IoT devices are sensitive and should only be accessible to authorized individuals. These applications are computer programs that use real-time or near real-time conditions. This ensures stable operation. The applications use consumer data to analyze and predict the future using artificial intelligence algorithms [1].

In 2014, the Joint Technical Committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) defined IoT as an infrastructure of objects, people, systems and information resources, connected between each other by intelligent services that enable them to process and respond to information from the physical and virtual world. At the IoT receiving layer, sensors placed inside devices, objects, and equipment collect, measure, and record information about the physical environment, such as temperature, humidity, gas pressure, and motion. This information can be read, integrated and analyzed at the upper levels of IoT [2].

NIST uses two acronyms: IoT and NoT (aka Network of Things). IoT is considered a subset of NoT because IoT has its "things" connected to the Internet [3]. In contrast, some types of NoT use only local area networks (LANs), and none of your "things" need to be directly connected to the Internet.

The growth of the Internet of Things is driven by business needs as part of digital business transformation. The total number of connections to the Internet of Things will grow from six billion in 2015 to 27 billion by 2025. This translates to a compound annual growth rate (CAGR) of 16%. In terms of market growth, the Berg Insight report forecasts the global market for third-party Internet of Things platforms to grow from 610 million euros in 2015 to 3.05 billion euros in 2021 [4].

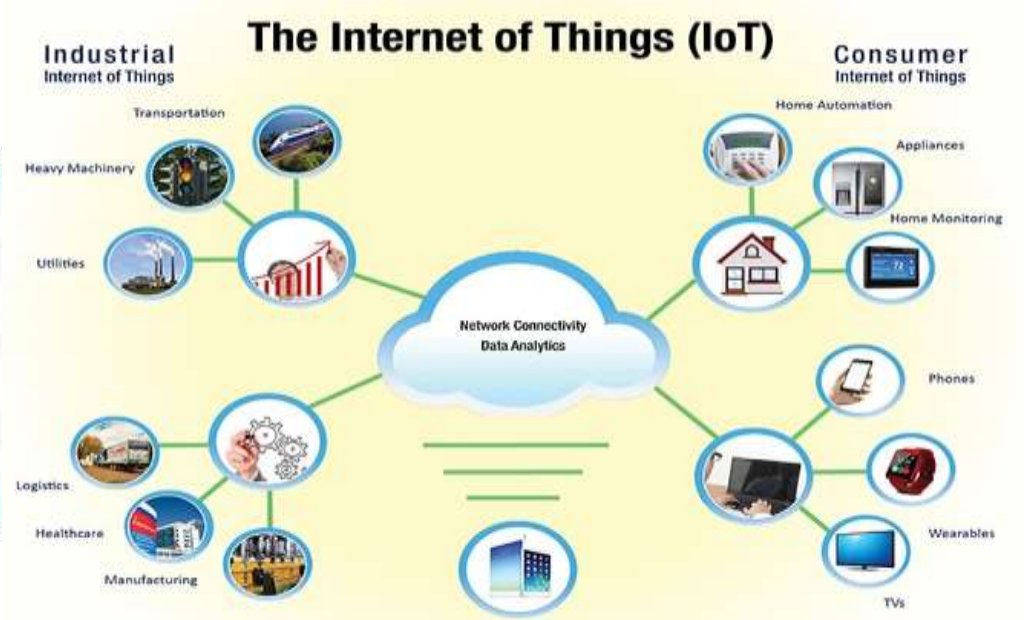

Figure 1. - Relation of the Internet of Things to industries

IoT solutions not only include several technology domains such as mobile, cloud, data, security, telecommunications and networks, but also lead to cross- industry use of data, e.g., data created in smart home and industrial applications are used in the automotive industry as shown in Figure 1 [5]. This opens up the possibility of trade associations between horizontal industries, such as telecom operators, and vertical industries, such as car manufacturers, as new business models.

The security of the Internet of Things must include more than just the IoT device itself. Internet of Things devices have minimal security and many defects. Many believe that IoT vendors do not prioritize security and privacy. But despite the security concerns, the proliferation of the Internet of Things is not stopping. Therefore, it is absolutely essential that security professionals and users learn how to provide greater security.

IoT Security Threats

A. Threats and security challenges of the Internet of Things

The three categories of threats to the Internet of Things include:

1. Typical risks in any online system.
2. Specific risks of IoT devices.
3. Safety to prevent damage, e.g. due to misuse of actuators [7].

Traditional security methods, such as blocking open ports on devices, fall into the first category (e.g., a refrigerator connected to the Internet to send product and temperature information may use an insecure SMTP server and could be compromised by a botnet).

The second category includes issues specifically related to IoT hardware, for example, a connected device can compromise your secure information. Some Internet of Things devices are too small to support proper asymmetric encryption. In addition, any device that can connect to the Internet has an integrated operating system implemented in its firmware, and many of these integrated operating systems are not designed with security as a primary consideration [8].

IoT is a collection of Internet-connected devices that collect and exchange data using nodes and controllers. The Internet of Things can be defined as a network of identifiable physical objects or "things" that can interact with each other, with the external environment, or both. With controllers and cloud processing, these devices can "think" and act autonomously and collect information for several reasons. A property of many "things" is full integration with or without an operating system (OS).

IoT basically collects data in real time using all types of networks (Local Area Network (LAN), Low Power Wide Area Network LPWAN), cellular LPWAN (Narrowband IoT and LTE-M) and cellular) with constant or intermittent connections to the cloud. Therefore, it is necessary to store time-stamped data, measure physical parameters, and be able to make decisions based on the data collected by these devices. This is necessary to achieve automated decision making in a centralized way [9].

Б. IoT security threats and attacks

There are four possible ways a security threat can occur on the Internet of Things:

- Physical attacks,
- Attacks,
- Software attacks,
- Cryptanalysis attacks.

Today's Internet of Things platforms are built using technology solutions from a wide variety of vendors. Some of these platforms are an eclectic mix of reused components from existing solutions for use on purpose-built platforms with the expectation that the

components will work together securely. Security measures in IoT components, if they exist, have not been designed to count the dependencies resulting from IoT connectivity. For example, industrial devices often lack proper authentication mechanisms because they are designed to be used in physically secure and isolated environments. Another example - problem timely providing updates software or security patches for end nodes without compromising functional security [10].

Complete risk and threat analysis methods and IoT platform administration tools are required. Developing mitigation plans for IoT attacks requires an understanding of the types of attacks and the sequence of actions that occur when they occur. Let's start by looking at the categorization of Internet of Things attacks. Analyzing security attacks helps us understand the real-world view of how the Internet of Things creates networks, and this allows us to define mitigation plans.

B. Categorizing attacks at the stages of the IoT process

In general, the IoT process can be viewed as a five-phase sequence: from data collection to data delivery to end users. The variety of attacks is categorized into five IoT phases:

- data perception,
- storage location,
- intelligent processing,
- information transfer,
- end-to-end delivery.

Г. IoT security requirements

Security needs to be addressed throughout the entire IoT lifecycle, from initial design to service launch. For example, implementing security features should start during device manufacturing. Code signing and code obfuscation are some steps that manufacturers can follow to ensure that your device is not hacked or an attacker does not insert unwanted code. Basic security requirements in Internet of Things scenarios include privacy and trust in data.

Д. Privacy of the Internet of Things

Maintaining privacy in the IoT remains a major challenge. Privacy refers to the protection of personal information as well as the ability to control what happens to that information. Privacy concerns with IoT systems are complicated by the fact that a system is more than the sum of its parts. Privacy considerations for low-level devices may be different from those at the data analytics level. At the same time, privacy breaches at any level of the system affect the entire system. A lot of private information can be collected from smart devices. In current Internet of Things technologies, there is little control over this information. In many cases, data is collected passively, and because of this, some privacy breaches may go undetected for long periods of time.

The core issue of IoT data ownership - who owns and controls what data, where that data goes - poses important regulatory, ethical and financial challenges. End users believe own all data. Producer source groups believe they own the data generated by their endpoints, or at least have access rights to it. In many cases, service providers believe they own the data as well as the application. Provider data ownership issues are becoming more complex as the Internet of Things becomes more heterogeneous. Systems with many participants from different organizations have been implemented. On old disassembled and unused devices everything still can store a lot of it sensitive information, and data sanitization is necessary for them. [11]

For example, a user's refrigerator reports the stock of food you eat and your fitness bracelet transmits your activity data, aggregating these data streams provides a much more detailed and sensitive description of a person's overall health. This type of data collection is becoming more common on consumer devices such as artificial intelligence TVs and personal assistant devices. These devices have voice recognition or "vision" features that allow them to continuously listen to conversations or observe activity in a room and selectively transmit data to a cloud service for processing, which sometimes involves a third party.

E. Opportunities

The goal of the Internet of Things is to improve the quality of life and provide benefits to consumers and businesses. The Internet of Things helps to achieve the following:

- Reduced energy consumption
- Safety and security improvements
- Improvements in the automation of everyday tasks
- Improving the quality of life

In this context, the implementation of the Internet of Things can be categorized into five types:

1. Industrial Internet of Things: facilitates better customer service by better customizing products and services for customers in a shorter timeframe. Improved connectivity and communication between assembly line and production, made possible by the IoT, allows manufacturers to be closer to market demand and customize then,that they build, according to the needs of their customers (e.g., smart factory) [12].

1. Commercial Internet of Things: includes smart commercial buildings.

2. The Internet of Things in healthcare: improving patient care. For example, IoT devices connect patients with healthcare systems to continuously monitor medical data. Patients can share their data with doctors, nurses and family members, as well as with machines and algorithms that provide automated feedback on the processed data.

3. Transportation Internet of Things: monitors the status of freight vehicles and

takes preventive measures during transportation if necessary. For example, IoT devices can track packages from start to finish to determine temperature, location, etc.

4. Consumer Internet of Things: connected consumer devices, including smart TVs, smart speakers, toys, handheld devices, and other smart devices.

Conclusions

This paper presents an overview of security threats to the Internet of Things in terms of recent developments, solutions to address them, and new technologies in development. It shows the paramount importance of security in developing viable Internet of Things solutions. Hopefully, this article will help you select secure Internet of Things technologies for your organization.

The application of IoT technology creates opportunities and risks for security, so the challenges with IoT devices regarding security are enormous. A thorough security risk assessment should precede any implementation to ensure that Detecting all relevant underlying issues. Without sufficient security and data protection, the IoT will not be successful in the long term. Therefore, it is a challenge for every Internet of Things manufacturer to complement all stages of the development processes, up to the operation of the equipment, with appropriate security measures. In future work, it is important to develop a framework for performing and assessing security risks in IoT to guarantee confidentiality, integrity and availability.

Literature

1. Tanweer A. A Reliable Communication Framework and Its Use in Internet of Things (IoT). 2018. №3. pp. 1-8.
2. Ryan P.J., Watson R.B.. Research Challenges for the Internet of Things: What Role Can OR Play? Systems. 2017. 5(1). pp. 1-24.
3. Kupriyanovsky V.P., Schneps-Schnappe M.A., Namiot D.E., Seleznev S.P., Sinyagov S.A., Kupriyanovskaya Y.V. Web of Things and the Internet of Things in the Digital Economy // International Journal of Open Information Technologies. 2017. №5. URL: cyberleninka.ru/article/n/veb-veschey-i-internet- veschey-v-tsifrovoy-ekonomike
4. Wegner P. Global IoT market size grew 22% in 2021. IoT Analytics. 2022. URL: iot-analytics.com/iot-market-size
5. Gloukhovtsev M., IoT Security: Challenges, Solutions & Future Prospects. 2018. C. 1-44.
6. Kumar S., Tiwari P., Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data. 2019. 6(111).
7. Tawalbeh L., Muheidat F., Tawalbeh M., Quwaider M. IoT Privacy and Security: Challenges and Solutions, Applied Sciences, 2020, pp. 1-17.
8. Polat G. Security Issues in IoT: Challenges and Countermeasures. Isaca journal. 2019. pp. 1-7.

9. Mentsiev A.U., Pakhayev H.H., Aigumov T.G. Security Threats of Narrowband Internet of Things and Countermeasures // Engineering Bulletin of Don, 2021, No.10. URL: ivdon.ru/en/magazine/archive/n10y2021/7249
10. Mentsiev A.U., Chebieva H.S. Modern threats to security on the Internet and countermeasures (review) // Engineering Gazette of Don, 2019, No.3. URL: ivdon.ru/en/magazine/archive/N3y2019/5859