DOI: 10.23977/jeis.2024.090211
ISSN 2371-9524 Vol. 9 Num. 2

Analysis of Security Vulnerabilities and Threats of Intelligent Devices in the Internet of Things and Countermeasures

Kerui Liu

Chengdu University of Technology, Chengdu, Sichuan, 610000, China
15908298182@163.com

Keywords: Internet of things; Intelligent equipment; Security vulnerabilities; Data encryption; Communication security

Abstract: This paper aims to deeply analyze the security vulnerabilities and threats of IoT smart devices, and put forward effective countermeasures. Through systematic research and analysis, this paper first summarizes the development and popularization of IoT smart devices, and emphasizes the importance of IoT security in today's society. Then, the common types of security vulnerabilities in IoT smart devices and their causes are analyzed in detail, as well as the impact of these vulnerabilities on IoT systems. At the same time, the article also reveals the serious consequences of major IoT security vulnerabilities. After deeply discussing the threats faced by IoT smart devices, this paper puts forward a series of specific strategies and suggestions, including strengthening identity authentication and access control, regularly updating and repairing security vulnerabilities, strengthening data encryption and communication security, establishing a sound security audit and monitoring mechanism, enhancing users' security awareness and education, and calling for the support and improvement of policies and regulations. In order to provide valuable reference and suggestions for manufacturers, users and policy makers of IoT equipment, and jointly promote the safe development of IoT industry.

1. Introduction

With the rapid development of science and technology, Internet of things (IoT) smart devices have penetrated into every aspect of our lives [1]. From smart home to industrial automation, from intelligent transportation to telemedicine, the application of IoT intelligent devices is increasingly widespread [2]. They interact with the external environment through various sensors and actuators, and realize data collection, analysis and remote control, which greatly improves the convenience and efficiency of life and work [3]. However, this popularity has also brought new security risks.

The security of IoT devices is very important to protect personal privacy, corporate assets and national security [4]. IoT devices are usually connected to the Internet, and many devices have remote control function, which makes them easy to be targets of hackers [5]. Once these devices are attacked, it may lead to data leakage, malicious control of devices, and even paralysis of the entire network system [6]. Therefore, it is of great significance to study the security vulnerabilities and threats of IoT smart devices for ensuring social security.

The purpose of this study is to deeply analyze the security vulnerabilities and threats in IoT smart devices, and put forward effective coping strategies through systematic research and analysis to enhance the security of IoT systems. It is hoped that this study can provide valuable reference and suggestions for manufacturers, users and policy makers of IoT equipment.

2. Overview of IOT smart devices

IoT smart devices refer to devices that can automatically collect, process and exchange data through network connection. These devices are equipped with various sensors and actuators, which can sense environmental information and perform corresponding operations [7]. IoT smart devices have a wide range of applications, including but not limited to the following aspects in Figure 1:

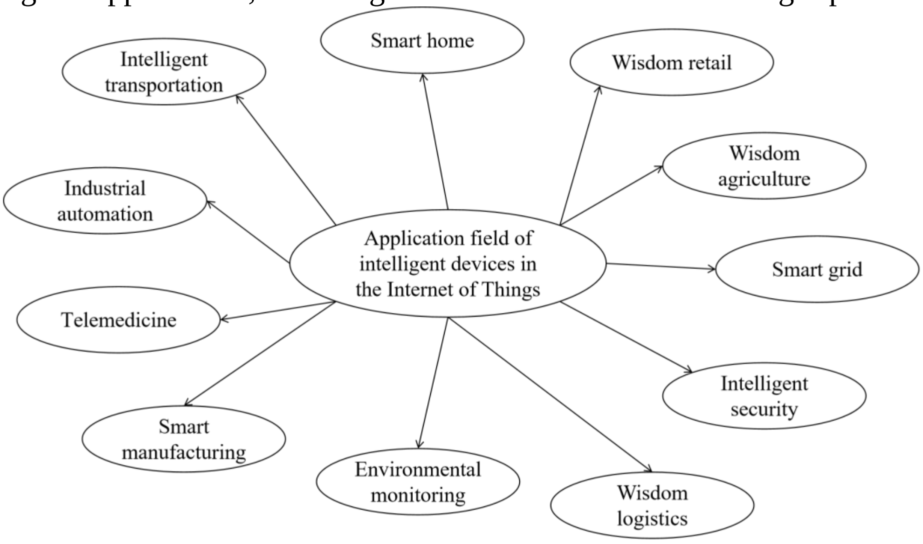

Figure 1: Application fields of IoT smart devices

The working principle of IoT smart devices is mainly to interact with the external environment through built-in sensors and actuators. Sensors are responsible for collecting environmental information, such as temperature, humidity, illumination, etc., and actuators perform corresponding operations according to control instructions, such as switching on and off lights and adjusting temperature [8]. These devices upload data to the cloud or server for processing and analysis through network connection, so as to realize remote monitoring and control of the devices.

The characteristics of IoT intelligent devices mainly include intelligence, networking, automation and interoperability [9]. They can independently perceive the environment and respond, and realize the remote transmission and control of data through network connection, which improves the automation and convenience of equipment.

3. Security vulnerability analysis of IoT smart devices

Common types of security vulnerabilities in IoT smart devices mainly include:

Authentication vulnerability: IoT devices may have problems such as weak password, unchanged default password or imperfect authentication mechanism during authentication, which makes it easy for attackers to gain control of devices.

Firmware update vulnerability: There may be problems such as unencrypted transmission, failure to verify the integrity of the firmware or failure to verify the secure firmware signature during the firmware update process of the device, which may lead to malicious firmware being installed, thus controlling the device or stealing data.

Input verification vulnerability: If the IoT device does not have sufficient input verification when processing user input, it may lead to security problems such as SQL injection and cross-site script attack.

Unsafe network communication: If the device does not use encryption or the encryption strength is not enough, the data may be intercepted or tampered with.

Privilege elevation vulnerability: An attacker may use the privilege management vulnerability in the device to elevate his own privilege, thus performing unauthorized operations.

There are various reasons for security vulnerabilities, mainly including the following aspects in Table 1:

Table 1: Causes of security vulnerabilities

Cause category	Detailed reasons	Example
Design defect	Potential safety hazards existing in the design stage of equipment. It may be due to the designer's lack of safety awareness or the neglect of safety in pursuit of function. This defect may be structural or strategic.	A smart device is not designed with user authentication mechanism, so that anyone can easily control the device.
Implementation error	In the process of software development, programmers may be negligent, have inaccurate understanding of requirements or have insufficient technical level, resulting in loopholes in the code they write. These vulnerabilities may be exploited by hackers to attack the system.	A common programming error is buffer overflow, which may lead to the execution of malicious code or system crash.
Improper configuration	During the installation and configuration of the equipment, if it is not operated according to the best practices or safety guidelines, it may leave potential safety hazards. This is usually caused by the negligence or lack of relevant knowledge of the administrator.	When a server is installed, unnecessary services are not turned off, or a strong password policy is not set, which may lead to security vulnerabilities.
Lack of updates and maintenance	IoT devices need to be updated and maintained regularly to keep their security. If it is not updated for a long time, the device may be exposed to known security threats, because these threats may have been exploited and published by hackers.	A router has not updated its firmware for a long time, which leads to hackers using known vulnerabilities to attack.

Security vulnerabilities have a far-reaching impact on the IoT system. It may not only lead to data leakage, but also make attackers have the opportunity to steal sensitive data such as user privacy information and device control instructions. It may also cause devices to be remotely controlled and perform malicious operations, such as turning on or off devices without authorization, and even tampering with device settings. In addition, attackers can also use some vulnerabilities to launch denial-of-service attacks, which will cause the equipment to fail to operate normally, thus seriously affecting the availability of the system. More seriously, because IoT devices are usually interconnected, the vulnerability of one device is likely to be exploited to attack other connected devices, thus posing a security threat to the entire network system.

4. Threats to IOT smart devices

(1) Network attacks and malware threats

IoT smart devices face various attacks from the network, such as distributed denial of service attacks and phishing attacks. At the same time, malicious software may also invade devices through vulnerabilities, steal data or destroy system functions.

(2) Risk of privacy leakage

IoT devices often collect and process users' private information, such as location data and usage habits. If the device has security holes or is infected by malicious software, this information may be illegally obtained and abused.

(3) Risk of illegal control of equipment

Attackers may take advantage of the security vulnerabilities of IoT devices to remotely control devices to perform unexpected operations. For example, smart home devices may be turned on or off without the user's permission, and industrial control systems may be maliciously tampered with to cause production accidents.

(4) System availability threat

The normal operation of IoT devices is very important for the availability of many systems. Security vulnerabilities may lead to equipment failure or malicious exploitation, thus affecting the stability and availability of the whole system.

(5) Social engineering attacks and internal threats

In addition to technical threats, IoT devices may also face social engineering attacks, such as phishing emails inducing users to click on malicious links or download malicious software. At the same time, insiders may also use their knowledge of the system to destroy or steal data.

5. Coping strategies and suggestions

In order to deal with the security vulnerabilities and threats faced by IoT smart devices, this paper puts forward the following strategies and suggestions:

Organizations/Companies should strengthen the authentication and access control of IoT devices: Implement strict authentication mechanisms, such as multi-factor authentication, to ensure that only authorized users can access devices. At the same time, set reasonable access control policies to restrict access to sensitive data and functions.

The subject can be added like this: "Users should regularly update and fix security vulnerabilities: Establish a regular software and firmware update mechanism to fix known security vulnerabilities in time. At the same time, users are encouraged to update equipment software in time to reduce potential security risks.

To strengthen data encryption and communication security, organizations should use strong encryption algorithms to encrypt data, ensuring its security during transmission and storage. In addition, a secure communication protocol is adopted to prevent data from being intercepted or tampered with during transmission.

Establish a sound safety audit and monitoring mechanism by appointing a dedicated safety team: establish a safety audit system and conduct regular safety inspections on IoT equipment. At the same time, ensure the implementation of real-time security monitoring, enabling timely detection and response to potential security threats.

Efforts to enhance users' safety awareness and education: Enhance users' understanding of IoT equipment safety through education and training, so that they can better protect their own equipment and data security.

Support and improvement of policies and regulations: The government should formulate and improve relevant policies and regulations, standardize the safety standards of IoT equipment, strengthen the supervision of equipment manufacturers and service providers, and ensure the safety of IoT equipment.

6. Conclusions

After in-depth research, this paper summarizes the main security vulnerabilities and threats faced by IoT smart devices. Firstly, authentication vulnerability is a common problem in IoT devices, which may lead to unauthorized access and data leakage. Secondly, the firmware update vulnerability is also a problem that cannot be ignored. Malicious firmware may be installed on the device through this vulnerability, thus controlling the device or stealing data. In addition, manufacturers should note that input verification vulnerabilities, insecure network communication, and privilege escalation vulnerabilities are also common security vulnerabilities in IoT devices.

In terms of threats, network attacks and malware threats are the main risks faced by IoT devices. Attackers may take advantage of the above security vulnerabilities to remotely control devices, steal data or launch denial of service attacks. At the same time, the risk of privacy leakage is also an important threat, and the risk of illegal control of equipment and the threat of system availability cannot be ignored. In view of the above security vulnerabilities and threats, this paper has put forward a series of coping strategies. With the continuous development and popularization of IoT technology, new security vulnerabilities and threats will also emerge. Therefore, we need to continue to pay attention to the latest developments in the field of IoT security, and update and improve security policies in a timely manner.

References

[1] Chen Shihong, Huang Xiaoqin. Research on vulnerability detection technology of Internet of Things devices [J]. Information and Computer, 2022, 34(21):219-221.

[2] Liu Yang, Yu Zhun, Weng Changjing. Construction and Thinking of the Internet of Things Security System in Smart Hospitals [J]. Hainan Medical, 2023, 34(17):2548-2552.

[3] Lin Peiliang, Zhang Zebin. Network-level security and privacy control of intelligent security Internet of Things devices [J]. Electromechanical Engineering Technology, 2023, 52(7):252-254.

[4] Feng Chao, Chen Jiongyi, Zhang Bin. Security assessment and enhancement of remote binding process of smart home devices [J]. Information countermeasure technology, 2023, 2(3):18-34.

[5] Liu Xia, Wang Yunfu, Jiang Yuanshan, et al. Research and design of industrial Internet of Things terminal security solutions [J]. Internet of Things Technology, 2023, 13(2):102-104.

[6] He Zhijian, Zhou Jiang, Luo Yuezhi, et al. Research on intelligent monitoring of power supply safety of super high-rise building equipment based on Internet of Things technology [J]. Automation Application, 2023, 64(5):30-32.

[7] Zhan Dongyang, Yu Zhaofeng, Ye Lin, Zhang Hongli. Multi-level kernel access control method for Internet of Things device security [J]. Journal of Information Security, 2022, 7(6):116-125.

[8] Wen Xiangbin, Zheng Yuan. Algorithm Simulation for Cloud Security Credibility Detection of Internet of Things [J]. Computer Simulation, 2022, 39(5):225-228.

[9] Li Tao, Tian Yingjun, Ge Yangchen, Tian Yuan, jian li. Overview of firmware vulnerability detection in the Internet of Things [J]. Information Security Research, 2022, 8(12):1146-1155.