ISSN 2093-0542

ICONI

KOREAN SOCIETY FOR INTERNET INFORMATION

The 14th International Conference on Internet

(ICONI 2022)

Dec. 11-13, 2022, Landing Convention Center,

Jeju Shinhwa World, Korea

http://www.iconi.org

Proceedings of ICONI 2022

| Organized by |

Korean Society for Internet Information (KSII)

| Co-Organized by |

Korea Electronics Technology Institute (KETI)
Advanced Institute of Convergence Technology(AICT)

| Sponsored by |

HUAWEI

Analysis of Security Issues and Defense Techniques of IoT Devices

Khasanboy Kodirov, HoonJae Lee, Young Sil Lee*
Department of Computer Engineering, Dongseo University Graduate School
Busan, South Korea
Department of Information Security, Dongseo University
Busan, South Korea
Department of Computer Engineering, International College, Dongseo University
Busan, South Korea
[e-mail: hasanboyadams@gmail.com, hjlee@gdsu.dongseo.ac.kr, youngsil.lee0113@gmail.com]
*Corresponding author: Young Sil Lee

Abstract

The Internet of Things (IoT) refers to technologies that enable devices to communicate globally by exchanging data over the internet and making decisions based on that data. IoT and IoT device-related technologies have grown quickly over the past decades. However, the fact that IoT devices are network-attached general-purpose computers that could be exposed to cybercrime has forced security countermeasures to keep pace. Many factors make IoT security critical today. Although IoT devices are a huge part of the discussion of IoT security, focusing only on this aspect of IoT does not reveal why security is important or what it involves. For this reason, in the field of IoT security, there are plenty of problems begging for solutions, including privacy protection and information processing security, malware risks, software and firmware vulnerabilities, insecure communications, and data leaks. This paper discusses the current IoT security issues and threats and proposes several possible defense techniques and how they can be achieved.

Keywords: Internet of Things, IoT security, IoT device security, IoT devices protection

1. Introduction

The Internet of Things (IoT) is a cutting-edge technology which involves a network of interconnected objects which are equipped with any type of digital machinery such as sensors, software and other technological elements. These objects can easily exchange data in real-time with other devices which are connected via networks. IoT devices are able to exchange data through a network without the need for human interactions such as human-to-human, or human-to-computer. A thing, in the field of Internet of Things, could be any object which has an Internet Protocol (IP) address and can transmit data over a network, such as a person who has a sensor inside the body to monitor the heart, an animal with a GPS tracker chip, or an automobile with sensors which can alert the driver if tire pressure is low. As wireless technology becomes more prevalent, computer components become smaller and cheaper, and IPv6 addresses become more widespread, this capacity can be used for almost anything. Aside from dedicated computing devices such as PCs, notebooks, smartphones and tablets, the possibilities are almost endless. For instance, in a variety of industries, organizations are using IoT to operate more efficiently, provide enhanced customer service, improve decision-making, and enhance their business value.

This research was a part of the project titled 'Marine digital AtoN information management and service system development(2/5) (20210650)', funded by the Ministry of Oceans and Fisheries, Korea.

According to IoT Analytics, it is estimated that there will be approximately 27 billion Internet-connected devices in use around the world by 2025[1]. All those IoT devices pose a big question: can tech companies protect them all?

2. Designing Secure IoT Structure

It is very important and highly recommended to carefully design the IoT security structure in the beginning of device production since the most fundamental way to mitigate IoT risks is to build security layers into into its structure. We can divide IoT security into 3 layers: the security application layer, the security network layer, the security perception layer (**Fig. 1**).

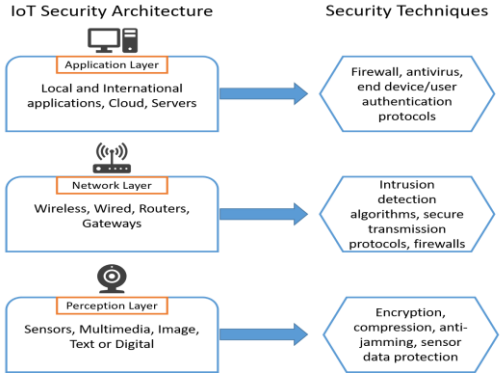

Fig. 1. IoT Security Design and Protection Requirements

Application layer security begins with a variety of security mechanisms, including selective disclosure, authentication, authorization, intrusion detection, firewalls, and antivirus. Next, the network layer must ensure security techniques that should be used on wired channels are firewalls, router control, resource multiplication, routing frills, and congestion control. Finally, the perception layer requires security techniques such as multimedia compression, encryption, timestamping, time synchronization, multimedia session identification, image compression, cyclic redundancy check, encryption, compression, and anti-jamming.

3. IoT Security Issues

Having insecure IoT devices poses a threat to the viability of networks, devices, systems, and users. It is possible to find IoT security vulnerabilities in almost everything from smart cars and smart grids to watches and smart home devices. A potential data breach can be caused by the challenges listed below when using IoT devices.

A. Lack of encryption

It is necessary to encrypt sensitive data that is stored on a device. Lack of encryption is a common weakness when API tokens and credentials are stored in plain text. There are also problems associated with using weak cryptographic algorithms or unintentionally using cryptographic algorithms.

B. Software vulnerabilities

In some cases, bugs in software may enable the device to carry out tasks for which the developers did not plan. As a result, the cybercriminal could be able to get hold of important information from the device or attack other parties.

C. Inadequate physical security

There is a high possibility that each physical device is vulnerable to tampering from the moment it is manufactured. When the hardware is poorly designed, an attacker might be able to insert malware into the USB port or hack the device through radio waves. Many years may pass before certain IoT devices are removed from use. As technology develops, an outdated device made with outdated technologies may eventually become more vulnerable.

D. Insufficient authentication and authorization

Although the system is protected by encryption and has secure hardware, it is still susceptible to be compromised. It is sometimes the weak strategy enterprises take to manage password authentication that leads to the problem. Many organizations still rely on the outdated method of resetting passwords after a certain length of time. Nevertheless, this does not take into account whether the password is strong, unique, or has been compromised previously.

4. Solutions to Secure IoT Devices

A. Strong encrypted communication

In order to protect users' privacy and prevent IoT data breaches, data at rest and in transit between IoT devices and back-end systems should be

encrypted using standard cryptographic algorithms as well as encrypted key lifecycle management processes in order to enhance user privacy and security generally. Information that is encrypted will remain private and confidential, regardless of whether it is stored or sent. According to Arcserve, the National Institute of Standards and Technology (NIST) is considering quantum cryptography in the future of encryption [2]. If IoT companies use this highly sophisticated encryption system, it would make it almost impossible for cybercriminals to exploit the system.

B. Secure APIs

APIs are often used by IoT devices to get data from other systems and share it. In order to prevent hackers from breaking into IoT devices that are weakly configured or unauthenticated, organizations need to comply with API security best practices and conduct continuous security testing. In order for data to remain secure while in transit or stored between a cloud, local network, and devices, all security standards and protocols need to be in place.

C. Comprehensive access control

An IoT device's services should only be accessible to the owner and those near them whom they trust. Unfortunately, this is not adequately enforced by most security systems. Due to hackers' constant efforts to gain access to personal information, full authentication can reduce IoT device vulnerability. Multifactor authentication, digital certificates, and biometrics are among the authentication mechanisms available for IoT devices.

D. EDR Security

The Endpoint Detection and Response (EDR) or Endpoint Detection and Threat Response (EDTR) solution continuously monitors endpoint devices, detecting and responding to cyber threats such as ransomware and malware. In addition to coordinating alerts and responses to immediate threats, EDR security also collects, correlates, and analyzes endpoint data. Another key capability of EDR is its ability to detect suspicious activity in real-time and block it automatically. While human security teams cannot always respond immediately to an incident, EDR uses threat intelligence to identify suspicious activity on IoT endpoints and rapidly conduct an efficient response.

5. Conclusions

To sum up, as a result of its security shortcomings, IoT devices have become a target for a variety of attacks, both small and large. According to an article published by Digit News, IoT devices had to face more than 1.5 billion cyberattacks in 2021[3]. Therefore, in this paper, we focused on how it is crucial to protect IoT devices so as not to fall victim to cybercrime. Security should be a top priority from the earliest stages of IoT research and development. A company's configuration alone isn't enough to secure IoT because both users and administrators should collaborate on creating a secure environment. In terms of users, this means using basic security best practices, like blocking unnecessary remote access and changing default security passwords. In addition, as mentioned earlier, security analytics, encryption, and visibility should be a priority for device manufacturers. Consequently, as a collaborative force, all of these IoT users, admins and manufacturers can ensure IoT remains secure.

References

[1] H. Mohammad., “State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally,” *IoT Analytics*, Accessed October 15, 2022, https://iot-analytics.com/number-connected-iot-devices/.

[2] A. Curioni., “How Quantum-safe Cryptography Will Ensure a Secure Computing Future,” *World Economic Forum*, Accessed October 24, 2022, https://www.weforum.org/agenda/2022/07/how-quantum-safe-cryptography-will-ensure-a-secure-computing-future/.

[3] D. Paul., “IoT Devices See More Than 1.5bn Cyberattacks so Far This Year,” *Digit News*, Accessed October 27, 2022, https://www.digit.fyi/iot-security-kaspersky-research-attacks/.