Research on Security Protection Countermeasures of Internet of Things

Bin Tang1, *, Mengqi Yang2

1China People's Police University, Hebei Province, China
2People's Public Security University of China, Beijing Province, China

*Corresponding author e-mail: toynben@163.com

Abstract. This paper introduces some countermeasures of Internet of Things security protection in three parts. The first part introduces the common security countermeasures, the second part introduces a security structure model of the Internet of things, and the third part introduces the protection measures of Internet of things using IPv6 protocol.

1. Introduction

Since the commercialization of 5G in 2019, it has solved the network connection bottleneck that has restricted the development of the Internet of Things (IoT) for a long time. Only 20% of 5G is used for people to person communication, and 80% will be used in the Internet of Things. The main purpose of the Internet of Things is the Smart Link, applications such as: intelligent decision-making, community management, face recognition, thermal imaging, Intelligent license plate recognition, automatic matching of logistics information, smart home and so on. At the same time, it also faces an important threat, that is, the problem of network security, which is an important link that restricts the development of the Internet of Things. The Internet of Things network architecture can be divided into three layers: perception layer, network layer, and application layer. Each layer faces different threats.

2. Security threats and countermeasures at all levels

2.1. The perception layers

The perception layer mainly refers to the IoT terminals, and the main threats include: key information acquisition, unauthorized access, fake terminal nodes, malicious energy consumption, malicious code/vulnerability attacks, etc. The defense methods that can be taken include:

In the aspect of physical security, the anti-disassembly design is added to the terminal allowed by the structure to realize the protection functions such as forced disassembly and self-destruction. In the aspect of system security, we implement the terminal system access system [1, 2], formulate terminal security standards, test and evaluate the network access terminals, and restrict the terminals that fail to pass the evaluation to access the system. Depending on the shared key, security certificate, MAC address of endpoint or trusted root based on immutable hardware, and human authentication (such as user name, password, token or biometric), to determine whether the identity of the terminal devices can be accessed with a single authorization and whether the identity information can be forged. Human authentication can use the context-based authentication method [3]. The principle is: consider
the controller access point used by the user (to communicate with the IoT device), and associate the
device ID with the traffic between the communication, and the contextual factor with fingerprints as
the main factor is obtained. The contextual factors involved include: whether the device fingerprints
match, whether the user name and password is correct, whether the protocol is changed, whether the
login frequency is abnormal, whether the login time is abnormal, and whether the IP and MAC is
abnormal, etc.

In the operation and maintenance stage, the principle of least authority management and control is
adopted for the terminal, and the debugging function and other interface functions that may create
security risks is turned off. The system supports real-time state monitoring of the terminal, supports
the emergency protection disposition such as shielding access to the network, remote locking and
remote data erasing of terminals, provides remote upgrade service for the terminal, supports the
remote upgrade package push, mandatory upgrade and other functions, and timely repair terminal
security vulnerabilities.

2.2. The network layers
The network layer provides wide-area network connections for IoT terminals and IoT platforms and
background applications. Because the network is generally a public network provided by
telecommunications companies, and business users share wireless air channels, there are security
threats such as interception of transmission data, malicious data tampering, leakage of privacy
information, and conflicts in security policies in network interaction. The security design of the
network layer involves authorization and mandatory security policies, mainly the security of the
network equipment itself, the chain of trust and security policies during the transmission process. The
security protection of the network layer can be carried out from the following aspects:

The security network is designed to use lightweight cryptographic algorithms to design a
lightweight, efficient, and wide-connection two-way network access authentication mechanism,
provide end-to-end encrypted communication protection between the terminal and the service platform
for advanced security users to ensure the confidentiality and integrity of information transmission, and
establish network access control between the core network and the access network, the core network
and the business platform, establish abnormal traffic detection and flow cleaning, intrusion detection
system(IDS) and other boundary security protection mechanisms, thus at the network layer, a basic
network security protection system such as anti-tampering, anti-intrusion, and anti-virus is built.

2.3. The application layers
For the application layer, it is a common business system security problem, such as: information
leakage, cross site script execution (XSS), buffer overflow, SQL injection, weak password, design
flaws and other vulnerabilities. At this level, protection methods such as commercial scanners, open
source scanners, monitoring and early warning systems are already very mature.

The business application platform needs to build basic protection capabilities: it needs to
implement functions such as identity authentication, access control, security auditing, and security
monitoring to ensure the safe operation of the business platform itself. Boundary security protection is
carried out between the business platform of IoT and the core network, between the business platform
and the user information system, and realizes the controlled exchange of information between the
business platform and the user information system. The business platform itself provides data storage
protection, data transmission protection and data access control to ensure the confidentiality, integrity
and availability of the business platform data.

In most cases, IoT platforms run on public clouds and share cloud infrastructure with other cloud
tenants. In addition, IoT platforms are mostly directly connected to the Internet and may face security
threats from the Internet. The main security threats are DoS attacks, unauthorized access, malicious
code and vulnerability attacks, and privacy information leakage. The security architecture model of the
Internet of Things can be constructed to deal with it.
3. IoT business security architecture model

3.1. Access control and hierarchical management
Since the service platform supports the access of multiple terminals and the processing of multiple types of services, it is necessary to implement the divisional and hierarchical protection of services [4]. The business platform can be managed and controlled by divisions according to user levels, and illegal access and information acquisition between different divisions can be strictly restricted. The model implements hierarchical management and control of the Internet of Things business platform according to business types, and implements business resource configuration and access control according to business levels.

3.2. Situational awareness and threat protection
The Internet of Things service platform can realize the security situation awareness of the entire network, real-time status monitoring of all terminals and network elements, and prohibit illegal terminals from accessing the system. The IoT business platform can monitor business behaviors and prevent threats, support protocol analysis of business data, identify security attacks based on application protocols, and filter and restrict illegal business access. The business platform can perform big data analysis on the collected system business data, and perform threat identification, risk warning and emergency response to the system.

3.3. Security domain division
The system can be roughly divided into four security domains: sensory control security domain, network security domain, application security domain, and operation and maintenance security domain.

3.3.1. Sensory control security domain. The security domain is mainly to meet the information security requirements of perception objects, control objects and corresponding perception control systems. A two-way identity authentication mechanism can be used between the terminal and the background application, while the session key negotiation is completed, and the session key is used to complete the business data interaction process. Identity authentication is mainly used to prevent fake terminals or background applications from accessing real background applications and terminals, and to ensure the credibility of the subject and object of business data interaction.

3.3.2. Network security domain. This security domain mainly meets the information security requirements of IoT gateways, resource exchange domains and service provision domains. It mainly guarantees the authenticity and validity of data collection and preprocessing, the confidentiality and reliability of network transmission, and the privacy and verifiability of information exchange and sharing. Network security protection is mainly to ensure wireless access network security and transmission network security. Wireless access network security mainly relies on telecommunications companies to complete the two-way access authentication between base stations and IoT terminals. Transmission network security is mainly to ensure the security of the transmission channel between the IoT platform and IoT business applications. Traditional Internet security protocols include Internet protocol security (IPsec), secure sockets layer (SSL), and authentication and key agreement (AKA), etc.

3.3.3. Application security domain. The security domain mainly meets the information security requirements of the user domain, and is responsible for the security requirements of system user authentication, access control, and operation and maintenance management. At the same time, it needs to have a certain amount of active defense against attacks to fully guarantee the reliability of the system.
3.3.4. **Operation and maintenance security domain.** The security management functions of this domain are mainly key management, identity management, device management, security auditing, and user management. Key management mainly realizes data encryption and decryption, signature verification, and identity authentication. Identity management is mainly based on the IOT identification system to manage the IoT terminal identification. Equipment management is mainly to manage the parameter configuration and status collection of information entities with security management functions. The security audit is mainly to record the security behaviors and events in the system so that the security behavior can be traced afterwards. User management mainly refers to account management and access control functions for security system operation and maintenance managers. In addition, it is necessary to classify user accounts, control the permissions of accounts to access devices, and control the number of online users.

3.4. **One safety reference model as show in Fig. 1.**

![Figure 1. One safety reference model.](image)

4. **Protection of IPv6 network**

The IPv6 protocol instinctively supports the communication of ultra-large-capacity IoT terminals, and the security protection of the IPv6 IoT network has also become a key consideration. The IPv6 network uses a lightweight routing protocol: IPv6 over Low power Wireless Personal Area Network (6LoWPAN). 6LoWPAN is divided into Route-Over routing and Mesh-Under routing [5, 6]. The Route-Over routing mechanism mainly uses IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) protocol. The protection of IPv6 network is mainly in two layers.

4.1. **Network layer security protection**

In addition to the general security threats in network routing, the RPL protocol also has other security problems, such as selective forwarding attacks, sink attacks, witch and clone attacks, denial of service attacks, rank attacks, version attacks, partial repair attacks, neighbor attacks, etc. The countermeasures are as follows:

4.1.1. **Prevention methods to deal with confidentiality attacks.** The network attack occurs because the confidentiality of RPL is destroyed, so a strong session key can be established between the route initiating node and the responding node. Secondly, only after the verified and authenticated node is
associated, the route exchange is allowed. It can encrypt all the source and destination addresses of the entire original data packet.

4.1.2. Methods to deal with integrity attacks. The system should implement storage access control, compare with historical routing and topology data, provide specific public key-based authentication and authorization, perform link layer security authentication, and calculate time reliability with a certain counter algorithm to ensure the freshness of the message to prevent replay attacks.

4.1.3. Methods to deal with usability attacks. The system adopts a two-way authentication method for flooding attacks, and nodes have the function of verifying signatures and message encryption. For selective forwarding attacks, the same message can be multi-path routed through disjoint paths, or the next hop can be dynamically selected from a set of candidates.

4.1.4. Methods to deal with IPv6 LAN attacks. The system uses the unicast reverse path forwarding (URPF) method to perform unicast reverse route lookup to verify and filter data packets. The method is to check the routing table according to the source address of the data packet to determine whether the forwarding port is consistent with the ingress port of the data packet, so as to determine the validity of the source address of the data packet.

4.1.5. Methods to deal with DOS attacks. The system adopts the moving target defense (MTD) technology of address jump, which can restrict the attacker from finding and tracking the target and protect the location privacy of the device. The device adopts the lightweight IPv6 address hopping protocol based on Internet of Things (L6HOP) protocol to continuously change the IP address. There are 264 IPv6 address hopping spaces, the attacker cannot judge the law of address hopping and cannot attack the target node.

4.2. Application layer protection
The system uses homomorphic encryption (HE): to achieve "computable but invisible data". Homomorphic Encryption refers to an encryption algorithm that satisfies the properties of ciphertext homomorphic operations, that is, after the data is homomorphic encrypted, specific calculations are performed on the ciphertext, and then the obtained ciphertext calculation results are homomorphic decrypted, the decrypted data is equivalent to directly performing the same calculation on the plaintext data.

If a homomorphic encryption algorithm supports any form of calculation on ciphertext, it is called fully homomorphic encryption (FHE), if it supports partial form of calculation on ciphertext, for example, it only supports addition and multiplication or limited number of additions and multiplications, it is called semi-homomorphic encryption or partial homomorphic encryption, referred to as somewhat homomorphic encryption (SWHE) or partially homomorphic encryption (PHE). In real applications, semi-homomorphic encryption is mostly selected for use, encryption is used to implement limited homomorphic computing functions in specific application scenarios.

Specific application scenarios mainly refer to the use of homomorphic encryption in cloud computing or outsourcing computing, in order to avoid the security risk of passing plaintext data directly to the cloud server. First, the user encrypts the data using a homomorphic encryption algorithm and encryption key, and sends the ciphertext to the cloud server, the cloud server calculates the ciphertext according to the program given by the user when the plaintext of the data is not known. After that, the ciphertext calculation result is returned to the user, and the user uses the homomorphic decryption algorithm and decryption key to decrypt the ciphertext calculation result, and the result is equivalent to the result of the same calculation directly on the plaintext.
4.3. Improve network operation and maintenance capabilities

A reliable traffic monitoring system should be added to the system. Through the monitoring of abnormal traffic and in-depth analysis of data messages, it can find traffic violations and abnormal traffic, intercept and restore suspicious IP traffic, detect mobile access devices in real time, and provide intelligent alarms in time. The system should improve the log management and security audit system, record users’ online behavior throughout the entire process, record the entire process of each business terminal’s access to the application system and the complete operation log. Through intelligent identification and data analysis of users’ access to content, violations such as application abnormalities, unauthorized access, data abuse, intrusion attacks, etc., can be founded, and then the system must take timely disposal measures, quickly track and locate, avoid serious harm, close unnecessary remote service ports, repair weak passwords, and regularly conduct network security risk assessments to improve protection. It is necessary to establish a sound remote data backup storage system, establish a distributed file storage system, use geographic separation, improve the system and data resistance to catastrophic events through structured and unstructured databases, and use specific disaster recovery management mechanisms, to ensure that the normal operation of the application system can still be guaranteed to the maximum extent after various disasters occur.

5. Conclusions

As an important infrastructure for realizing the interconnection of everything and intelligent applications, the Internet of Things is listed by the world as a key task in the digital economy and social transformation, but the network security challenges it faces are also very serious. Now new protection technologies continue to emerge, such as blockchain solutions, the blockchain is decentralized, cloud servers and central servers are no longer needed for data processing, thereby security risks at the application layer will be reduced.

Acknowledgments

This work was financially supported by CPPU University Research Fund, research project number: ZQN2019025.

References

[1] Zhang Fan, Jiang Zisen, Zeng Yong, Chen Fuli, New Thinking on the Security Architecture of NB-IoT Internet of Things System, J. Communication Technology, 52(2019) 1987-1991.
[2] Fan Guolin, Zhu Shuangning, Jin Xiaoyan, Research on Internet of Things Security Protection Technology Based on NB-IoT Technology, J. Communication Technology, 53(2020) 1244-1249.
[3] Du Junxiong, Chen Wei, Li Xueyan, Contextual authentication method based on fingerprints of Internet of Things devices, J. Computer Applications, 39(2019) 464-469.
[4] Liu Bo, Chen Hui, Wang Haitao, Fu Ying, Analysis of Internet of Things Security Issues and Research on Security Models, J. Computer and Digital Engineering, 11 (2012) 21-24.
[5] Luo Yujie, Zhang Jian, Tang Zhangguo, Li Huanzhou, Overview of research on low-power lossy network security routing protocols, J. Computer Applications, 38(2018) 3462-3470.
[6] Huang Tinghui, Ding Yongxi, Li Sijun, Research on Lightweight Security Protocol of Internet of Things based on MT6D, J. Computer Engineering online edition, https://doi.org/10.19678/j.issn.1000-3428.0055664.2019.9.