Research on authentication encryption mechanism based on intelligent door lock vulnerability risk

Yili Lu*

Ministry of Transport Management Cadre College, Cyber Security, Beijing, China

Abstract. This article introduces the security risks of the commonly used MQTT protocol in the Internet of Things and the security risks caused by smart door lock vulnerabilities, aiming to solve the problem of public MQTT agent leaking smart lock data, causing attackers to use the sensitive data to physically locate and remotely control the connection to the smart door lock supplier Any lock issues in the cloud infrastructure. This paper presents a wireless sensor network authentication encryption method based on SM9 algorithm. By implementing and deploying sensor network authentication encryption in practical applications, it avoids the leakage of sensitive information from public data exposed on the Internet.

1 Introduction

In the current era of the Internet of everything, 5G, big data, artificial intelligence and other new technologies have brought innovative vitality to the Internet of things. The Internet of things is deeply integrated with personal and family life and industrial production, bringing profound changes to the whole society. In the era of "smart locks" of the Internet of things, unlocking tools are no longer crochets, but scripts and sniffers. Penetration testing experts have revealed the security threat behind a brand of Intelligent door Lock vulnerability: attacker can physically locate and remotely control any lock connected to the cloud infrastructure of the Intelligent door Lock provider.

Wireless sensor network (WSN), which is the core component of the perception layer of the Internet of things (IOT), is more and more widely used in military, environmental protection, medical and many other fields. Because of the openness of WSN, attackers are easy to capture nodes and launch attacks internally, so authenticated encryption is needed to deal with this attack. This paper presents an authenticated encryption method based on identity cryptography mechanism (Identity-Based Cryptography, referred to as IBC). The purpose of this paper is to study the hidden risks of intelligent door locks caused by vulnerability risk in MQTT protocols commonly used in the Internet of things, and encrypt the MQTT public data transmission data exposed on the Internet through IBC authentication encryption method, so that attackers cannot view sensitive information in data even if they obtain MQTT public data. After successfully using this encryption authentication for door

* Corresponding author: luyili@motmti.cn

locks, it can be extended to many IoT application scenarios, such as smart cities and driverless cars.

2 Introduction security risks of MQTT protocols commonly used in the Internet of things

The physical structure of the Internet of things includes physical devices, message forwarding middleware, back-end servers, and front-end control devices.

Physical devices are objects that need to be monitored and controlled in the Internet of things, such as intelligent door locks, vehicles, street lamps and so on. The object connects to the Internet through a sim card, sends real-time data of the current equipment to the Internet, receives control commands from the Internet, and completes command operations through physical devices such as relays.

Message forwarding middleware is a middleware tool for physical devices to connect to the Internet, which is commonly connected with MQTT protocol. A MQTT middleware is built on the server side. The specific equipment completes message delivery by subscribing and publishing specific channels.

The back-end server is the web server that provides data query. The server side is responsible for data storage, synchronization, authority control, providing data interface, command interface, completing data analysis and other tasks.

The front-end control device is the display end and the control end, which is the closest to the user, providing the user login interface and user equipment list, and the user can monitor and control the devices with permission.

The network structure of the Internet of things is mainly divided into three layers: perception layer, network layer and application layer. The sensing layer includes various sensing devices. The network layer includes the access network and the core network. The application layer includes a common platform for providing basic services and business application systems involved in various fields on the platform.

MQTT is an agent-based publish-subscribe protocol, which works on the application layer protocol of the TCP/IP protocol. The message agent is responsible for coordinating the local data exchange between the connected nodes. There are many MQTT application scenarios. These sensors and actuators are low-power IoT components connected to the MQTT agent. The sensor publishes data and the monitoring application subscribes to this data, and sends commands to the actuator. Sensor data is published using descriptive and hierarchical topic names.

When MQTT is deployed without proper authentication and authorization schemes, there is a risk that MQTT will be abused, and anyone connected to agent can obtain sensitive data and even control dynamic systems. Unauthorized users who have access to the MQTT agent can easily guess the topic name and subscribe to various topics using the # wildcard character to get the data of the transport agent.

By studying the exposed MQTT system, testers found numerous industrial Internet of things network risks, including vehicle tracking and taxi dispatching, such as hardware and software that did not update vulnerability patches in time, making these devices extremely vulnerable to attacks.;Using weak and default credentials and not regularly changing credentials, malware and racketeering software attack and lock consumers to use their own devices, requiring consumers to pay ransoms to recover their data; Internet of things devices need many types of applications, services and communication protocols, and the complex application scenarios of the Internet of things make it difficult to monitor, and many devices are hacked and continue to run without the user's knowledge; data protection and security challenges become very difficult because it is difficult to predict and prevent attacks, because it can be transmitted between multiple devices in a matter of seconds, One minute ago it is

stored on a mobile device, the next minute it may be stored on the network and then in the cloud; the smart home faces potential risks, once the IP address is exposed, the user's home address and other contact information will also be exposed; once hackers hijack and control the car, self-driving cars or cars using Internet of things services are very dangerous. Every day, a large number of Internet of things devices connected to the cloud without network security tests are on the market,We must be aware of this cumulative risk and strengthen the regulation and supervision of product network security.

3 Security problems caused by vulnerability risk of intelligent door lock

3.1 Disclosure of personal information by public MQTT data

The tester collects the smart lock data of the MQTT agent exposed on the public Internet, including the user email and IP address associated with the intelligent lock, as well as the timestamp records of the opening and closing of the intelligent lock.

The tester listens to the MQTT message sent by the intelligent lock through WIFI, and uses data such as e-mail address, local MAC address and public IP address associated with MQTT data for geographical location, which is sufficient to identify personal identity and home address. As long as you know the device MAC address, you can steal the "unlock token" and unlock the intelligent door lock in batch or at fixed point.

3.2 Improper access control settings lead to user name and password disclosure

Intelligent lock has taken a series of user authentication measures: close unauthenticated ports and user access, and add restriction rules to the subscription and delivery function to restrict unauthenticated users from subscribing to data.

The intelligent door lock does not implement user-level access control. By grabbing the MQTT traffic of the application and obtaining the MD5 summary of the device-specific user name and password, the tester can connect to and interact with any Intelligent door Lock user's device with any free / anonymous account.

4 Research on IBC authentication encryption mechanism based on security loophole of intelligent door lock

IBE is an encryption technology that generates a user key based on a user's identity. As the user's public key, the user's identity information (such as ID card number, phone number, physical address, etc.) does not need to be issued a public key certificate. In order to realize the identity authentication and data encryption transmission of the sensor in the intelligent door lock, the IBC key infrastructure is deployed in the application layer, each terminal entity applies for the IBC private key, and the authentication encryption is realized when the sensor is running, so as to ensure the security of the wireless sensor network.

4.1 Components of IBC key Infrastructure

IBC key infrastructure is mainly composed of key generation center, registry and local registration agent, public parameter service and terminal entity. This is shown in figure 1 below:

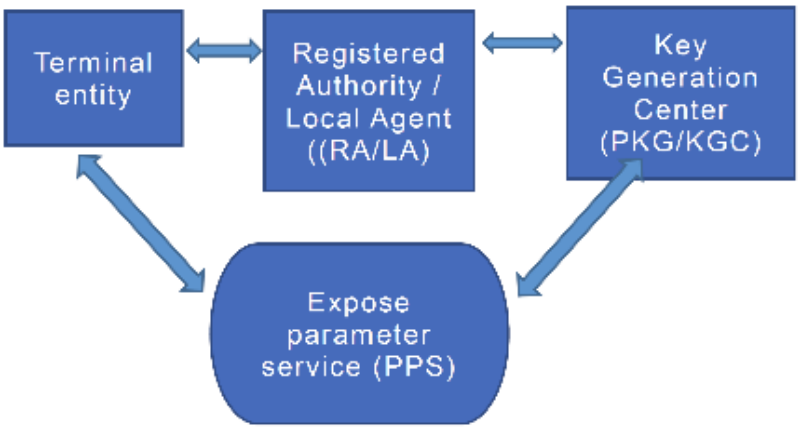

Fig. 1. IBC key infrastructure composition.

1.Key Generation Center (PKG/KGC): it is the core component of key infrastructure. KGC mainly includes the functions of key generation, key management and public parameter management.

2.Registration authority / local agent (RA/LA): RA is responsible for the acceptance and examination of local user registration applications, user private key application and download, and user registration security management. The local agent LA provides acceptance of registration applications for remote users.

3. the public parameter service (PPS): It is a public information service system that provides public password parameters, PKG policy information and user identification status query services.

4.Terminal entity: It is the software and hardware with IBC cryptographic operation module that represents the identity of the terminal, and realizes the storage and use of its own private key.

If the terminal entity such as the intelligent door lock applies to RA locally, if the terminal entity registers and applies for a key with the remote user agent LA remotely, the LA sends the user information to RA, RA transfers to KGC. After KGC receives the user key application, it generates the user private key based on the root private key and user ID, and transmits it to the entity user through the secure channel. According to the user identification and specification algorithm and parameters, the public key of the entity user can be generated by the communication related parties in real time to realize the secure communication between entities. The private key and system public key parameters are stored in the cryptographic machine. The key management facility is deployed in a distributed manner. The main PPS is configured in the core area, and the secondary PPS is configured in the application service area. The terminal entity and the key generation center can query the PPS in real time. Key parameter. This is shown in figure 2 below:

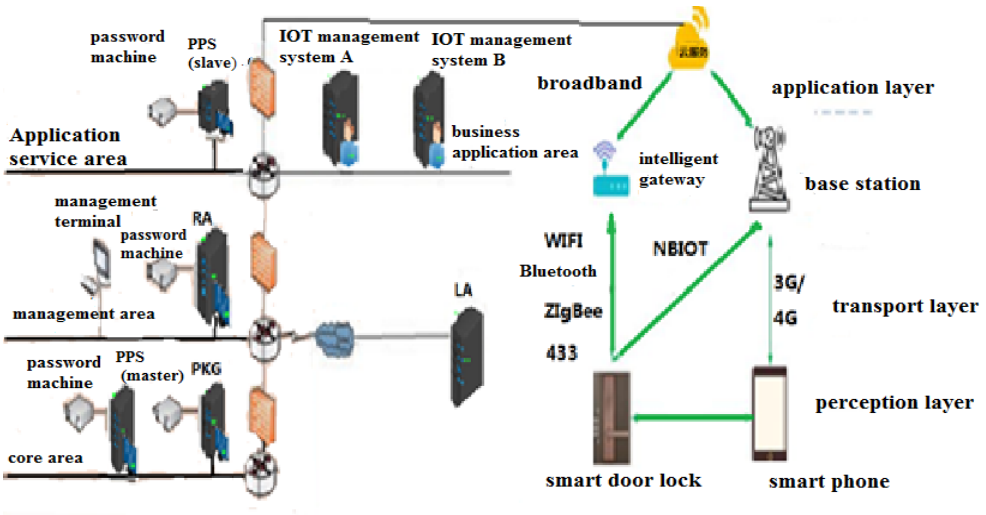

Fig. 2. Intelligent door lock sensor network structure based on IBC key management facility.

4.2 Authentication encryption mechanism in intelligent door lock sensor network

The authentication and encryption of intelligent door lock sensor network is based on IBC key infrastructure, which includes three steps: system initialization, identity authentication and data encryption, and key update.

4.2.1 System initialization

The initialization process of the system is mainly divided into four processes: initialization of IBC key management facilities, initialization of terminal sensor and IoT service management system, and release of terminal entity information.

The IBC key management facility initializes the system parameters generated by PKG, the public key of the system master key is public, and the private key is kept privately in the cipher machine. When initializing, the terminal sensor and the IoT service management system submit their own unique identification to PKG,PKG to calculate the user's public key and the user's private key, and write the private key and the public key into the cipher machine. The initialization of the system facilities is shown in Table 1 below:

Table 1. Initialization process of system facilities.

Initialization of system facilities	Identification	Public key	Private key	Storage
IBC key management facility	System parameter Params	P_{pub}	P_s	The public key is public and the private key is stored in the cipher machine.
Terminal sensor	ID_s (physical address, geographic	$Q_s=H(ID_s)$	$d_s=s \cdot Q_s$	The private key and public key are written into the cipher machine.

	location, system naming)			
IoT service management system	ID^{R} (identity certificate, IP, system name)	Q_g	d_g	Private key and system public key parameters are written into the cipher machine

Terminal entity information release: PKG publishes the sensor applying for key service and the service management system identification status to the PPS, service management system to query the sensor identification status from PPS.

4.2.2 Identity authentication and data encryption

Identity authentication includes two parts, one is the identity authentication between sensor nodes, and the other is the identity authentication of service management system and sensor gateway, which is realized by IBC signature verification algorithm.

In order to encrypt business data, a three-level key management system is adopted, including master key RK (Root Key), key encryption key KEK (Key Encryption Key) and session key SK (Session Key).

System master key RK: The identity public and private key Q_g d_g of the business management system and the identity public and private key Q_s d_s of the sensor node are both generated by PKG.

The identity public and private key of the business management system and the identity public and private key of the sensor node, both public and private keys are generated by PKG.

The key encryption key KEY:KEY key generation is negotiated between the service management system and the sensor gateway, and the KEK encryption protected by the node private key is distributed online to each node of the sensor network through the sensor gateway.

Session key SK: The business communication data between the business management system and the sensor node is protected by SK symmetric encryption, and SK is protected by KEK symmetric encryption. The business data encryption management process is shown in figure 3 below:

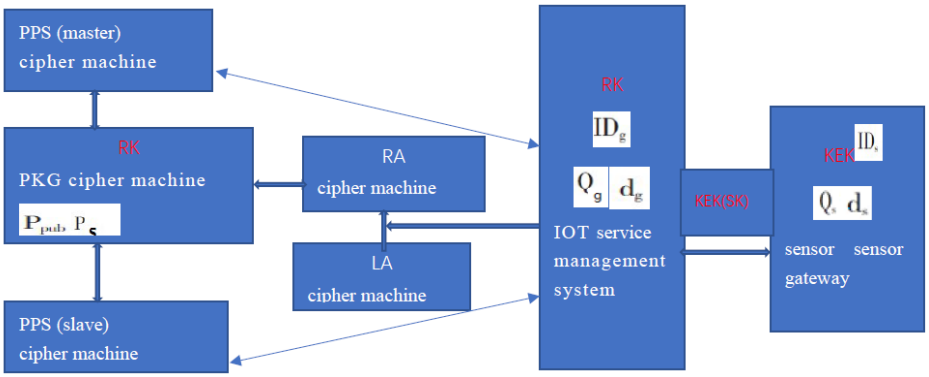

Fig. 3. Intelligent door lock sensing service data encryption management process.

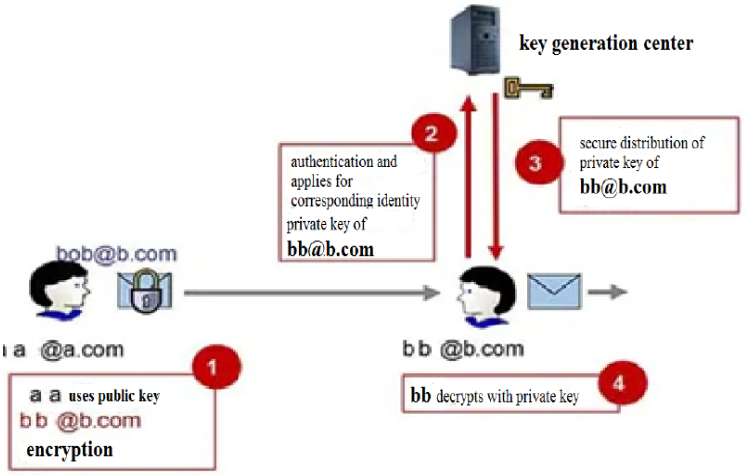

Fig. 4. Public key encryption and private key decryption process.

4.2.3 Key update

System master key RK update: generally update the identity key online through the key management facility. After the sensor node is deployed, the update node identity key cannot be updated online because the network is unreachable; generally, two pairs of identity public and private keys are generated when the sensor node is initialized, so that all nodes in the current domain disable the current identity public and private keys and enable another pair of identity public and private keys.

Key encryption key KEK update: the update is completed by negotiation between the service management system and the sensor gateway.

Session key SK update: real-time update, one secret at a time.

5 Conclusion

This paper describes the common security risks of the Internet of things ,and takes the security loophole of the intelligent door lock as an example, analyzes the exposed MQTT system, and finds that the intelligent door lock MQTT agent has the risk of being abused, which leads to the leakage of personal information data from the public MQTT data of the intelligent door lock.

Through the construction of IBC key infrastructure, we can achieve identity authentication between sensor nodes, sensor nodes and business management system in wireless sensor networks, encrypt business data, and improve the security of wireless sensor networks. The authenticated encryption mechanism in wireless sensor networks studied in this paper can deploy SM9 key infrastructure and encrypt business data through SM9 algorithm in practical applications. The scheme is achievable in practical application, and provides a reference scheme for the encryption algorithm transformation of sensor networks in the Internet of things.

Reference

1. Zhihao Yu, Li Ma, Chunping Hu, Internet of things Security Technology, Tsinghua University Press, 2016 (4).93-103

2. Multi-dimensional Security, an example of Smart City Security system-- is Intelligent door Lock secure , Gui Wei Security, 2018 (11) 1-2.
3. Security cow, Internet of things security crisis hidden by Intelligent door Lock, Security Internal reference, 2020 (8) 1-3.
4. Jiatao Lin, discussion on the Security of the Internet of things based on Cloud Computing, Network Security and Informatization, 2020 (7) 1-3.
5. Junyan Lin, Zhaolei Zhang, Zhiwei Yuan. Research on authenticated encryption Mechanism based on IBC in Internet of things, Information Security and Communication Security Magazine, 2020 (8) 95-101.
6. Chunxiang Xu, Haitao Xu, Wenyu Zheng, Research on Security Strategy of Internet of things based on Cloud Computing, Aixue, 2019 (2) 1-3.