Security system of Internet of Things based on Subscriber Identity Module

Xiaoming Ren1,a*, Zuhui Yue2,b, Zheng Li3,c
1China Mobile Research Institute, Beijing, 100053, China
2China Mobile Research Institute, Beijing, 100053, China
3China Mobile Research Institute, Beijing, 100053, China
arenxiaoming@chinamobile.com
byuezuhui@chinamobile.com
clizheng@chinamobile.com
*Corresponding author’s e-mail: renxiaoming@chinamobile.com

Abstract. There are many security issues in the IoT field and current security solutions can’t provide high security level and cost-effectiveness at the same time. This paper expounds the IoT security service architecture based on Subscriber Identity Module (SIM) card and the key technologies of the service, including bi-directional authentication, secure data transmission and local secure storage. At the same time, it also analyses two modes of the security services, namely simple service mode and self-service mode. With the benefit of SIM, the solution can become a preferred security solution which provides a high security, low-cost, fast implementation and high cost-effective service for the IoT industry.

1. Introduction
Since ITU published ITU Internet Reports 2005 [1] and formally proposed the concept of the Internet of Things in 2005, the Internet of Things has developed rapidly. And at the same time, security issues have become increasingly prominent, security incidents have also increased year by year and the losses are difficult to estimate. Among various security issues, weak identity authentication of IoT terminals and poor data transmission security are the main causes of risks. At present, some solutions can solve the above problems to a certain extent, such as solutions based on Secure Element (SE), TEE (Trusted Execution Environment) and security solutions based on software, etc. However, these solutions still have problems more or less. For example, the cost of SE solutions is relatively high, and it is difficult to popularize due to the cost-sensitive IoT terminals; the software solutions have low level of security. The industry urgently needs a solution that takes both cost and security into consideration.

The security service based on the SIM card is just such a solution. The SIM card is a natural trusted hardware on the cellular network terminal, with high security (same level as SE) and no additional cost. The basic security capability based on SIM card can provide security services such as identity authentication, data security transmission, local secure storage for IoT terminals, etc.

The SIM card has a natural advantage in the field of security services. It can be foreseen that with the promotion and popularization of 5G networks, security services based on the SIM card will be more and more widely used.
2. The current security status of IoT terminal

In recent years, the Internet of Things has developed rapidly. As of 2019, the number of global IoT device connections has reached 11 billion. According to GSMA's forecast, the number of global IoT terminal links will reach 25 billion in 2025 (as shown in Figure 1).

![Figure 1. Global IoT terminal connection data volume and forecast](image)

However, with the rapid development of the Internet of Things, security issues have become more and more prominent. There are a large number of IoT terminals with serious fragmentation, and a large number of IoT terminals are directly connected to the mobile Internet, which is easy to become the target of hackers.

According to the analysis of the security situation of IoT terminals in literature [2], the terminal security capabilities are generally low, leading to frequent occurrences of various security incidents, including denial of service attacks, unauthorized control of device, sensitive data leakage, etc. At the same time, IoT security incidents have a wide range of impacts, covering vertical industries such as smart healthcare, Internet of Vehicles, smart homes, smart cities, and smart meters. The key points of risks include:

- There are many types and large scales of terminals, which are difficult to be managed in a unified method. The lack of a unified standard for security solutions results in uneven security protection and shortcomings of various types of terminals in various industries.
- The security protection capability of terminals is low, and it is difficult to resist attacks. Among them, in terms of hardware security, the hardware lacks of sufficient protection and is easy to be damaged; In terms of firmware security, terminals generally have problems of weak identity authentication and authorization mechanisms, and lack the necessary security protection capabilities; in terms of communication security, there is no unified security protocol; In terms of application security, there are vulnerabilities which are easy to be exploited; in terms of data security, there are hidden dangers in the storage and transmission of sensitive data.

In summary, the IoT industry needs a terminal security solution with low cost, strong security, easy implementation, and broad coverage.

3. Introduction to IoT terminal security solutions

At present, the security solutions often used by IoT terminals can be roughly divided into two categories, namely, software solutions and hardware solutions.

The software solution is currently adopted by the vast majority of IoT terminals, which is also the fundamental reason of the low security capabilities of IoT terminals. Software solutions have low security levels and may have vulnerabilities. In the meantime, IoT terminals generally lack a safe and timely software update mechanism. These factors all lead to huge security risks in this solution.

The hardware solution is a security solution based on the security capabilities provided by the hardware security medium configured on the terminal. There are mainly two types of hardware, TEE
(Trusted Execution Environment [4]) and SE (Secure Element), which can be used for IoT security [3]. Compared with the software solution, the hardware solution has the characteristics of high security level, good performance, and easy maintenance, but this solution has also encountered resistance in the promotion process. For example, the use of a dedicated SE (the SE is designed to provide security capabilities for the terminal) means that the terminal needs to add additional security hardware in addition to business needs, leading to an increase in overall production costs, which also shuts out most end users of the Internet of things.

Literature [2] proposed a new idea of providing a security solution for IoT terminals, that is, it is recommended to use the endogenous security mechanism provided by the SIM card as a protection method for terminal security. This endogenous security is the inherent security capability of the SIM card. On the one hand, this solution is a hardware-based solution, which has the advantages of the hardware solution; On the other hand, it does not require additional hardware, which also makes the solution low-cost. Therefore, this solution provides an excellent choice for the security of IoT terminals.

4. Establishment of IOT security service system based on SIM card

4.1. Introduction to SIM card

SIM card is an authentication module inserted in various mobile Internet of Things devices to access the operator's network.

The physical form of the traditional SIM card is a plug-in card. In recent years, driven by market demand, a chip-shaped SIM card, namely eSIM, has been derived. Based on the functions of the traditional SIM card, eSIM adds the ability to dynamically download authentication data. (If not specified, SIM card in this paper covers both traditional plug-in SIM card and eSIM).

SIM card has the following characteristics and advantages:

- High level of security: SIM card integrates a security chip with a high security level. It can not only prevent software attacks from the network, but also protect against various physical attacks, and can be used as the root of trust for various devices.
- Multi-application support: Compared with other devices, the SIM card application management is more flexible. According to the needs, the SIM card multi-application management architecture based on international standards can be used to dynamically deploy secure applications in the SIM card, and perform comprehensive application and related data management in the whole life cycle.

In addition to the above advantages, since the SIM card is a necessary identity module to access the cellular network, and the security capabilities of the SIM card do not increase new hardware costs, therefore, for the IoT users, the SIM card is a cost-effective safe medium.

4.2. Security service architecture of Internet of things based on SIM card

The security service of IoT that is built into the SIM card uses the SIM card as the security carrier, relies on its high-security computing and storage capabilities, and combines with the cloud-side security service platform and key management system, to provide security protection of IoT terminal, identity authentication and data transmission protection between IoT terminal and platform for SP.

The overall architecture of the system is shown in Figure 2:
Figure 2. Security service system architecture of IoT based on SIM card

The IoT SP deploys the SIM card and the supporting terminal SDK middleware on the terminal side. The terminal side application can call the security service capabilities provided by the SIM card through SDK, including platform authentication, secure data transmission, secure data storage, etc. The cloud side security service platform can provide online security services, including terminal authentication, data secure transmission, etc. The key management system provides key management services for the security service system and secure SIM card issuance services. The IoT SP is connected to the IoT security service platform, and cooperates with the end-side SIM card to achieve end-to-end two-way authentication and secure data transmission between the IoT terminal and the SP platform.

In response to different IoT industries and different terminal needs, operators will issue SIM card products with different functions and configurations, including plug-in, embedded form, and consumer and industrial grade. At the same time, for different vertical industries, there will be SIM cards with different configurations. For example, for the Internet of Vehicles, it can provide high-performance SIM cards that meet the requirements of vehicle regulations, and for ordinary IoT terminals, it can provide SIM cards with common configurations. All types of cards can provide IoT security services.

4.3. The IoT security service technology based on SIM card

4.3.1. Bidirectional Authentication

Authentication is one of the core functions of IoT security services. The purpose is to ensure the authenticity of the identities of both parties in the information exchange. This service provides an end-to-end mutual authentication service between the device and the SP platform for the IoT SP through the secure interaction process between the SIM card and the IoT security service platform.

Key agreement is one of the core processes of authentication (it can also be said that authentication is the core process of key agreement), and it is also a key technical procedure that needs to be designed for IoT security services. The purpose of key negotiation is to use the keys and security parameters that the interacting parties already possess to obtain the unique security parameters and temporary keys of this session through the process of security interaction, so as to realize the security of the session. For some IoT terminals, due to their limited processing capacity and energy consumption, it is usually required to minimize the number of interactions, while the standard key agreement process requires multiple interactions. For the SIM card, it can combine its own characteristics to provide a counter-based secure interaction process. It can ensure security and reduce the number of interactions.

After the key agreement process, the negotiated key can be used to perform cryptographic processing on the session parameters and identity information, thereby implement authentication.

A typical scenario of bidirectional authentication for the Internet of Things is shown in Figure 3:
Among them, a legitimate IoT device can add authentication information to the business data and transmit the data to the IoT operator through the security capabilities provided by the integrated SIM card. The SP requests the IoT security service platform to authenticate the device. After the authentication is passed, the SP will accept the data, and illegal devices will not be able to forge the uploaded data.

For IoT devices that need to receive data sent by the platform (such as shared devices), the platform will apply for data authentication services to the security service platform before sending the data, and after adding the verification information of the platform, it will be sent to the device. The device verifies the data through the security capabilities provided by the SIM card. The data is received only after the verification is passed, otherwise it is rejected. Therefore, the illegal platform cannot forge the data and send it to the IoT terminal.

Through the above two-way authentication mechanism, platform authentication is realized for the terminal on the one hand, and device authentication is realized for the platform on the other hand.

4.3.2. Secure data transmission
Data security transmission meets the confidentiality and integrity requirements of the data transmission process. The session key negotiated between the SIM card and the IoT security service platform can be used to achieve the encryption, decryption and integrity protection of the interactive data. It can provide two-way data secure transmission services between the device and the SP platform for the Internet of Things SP.

In the process of data security transmission, the primary step is still key agreement, which has the same requirements as the authentication process. Using the characteristics and basic capabilities of the SIM card, it is possible to implement a counter-based key agreement process, and the key agreement process is implicit in the process of data secure transmission, thereby greatly reducing the number of interactions and improving transmission efficiency.

A typical scenario is shown in Figure 4:
In this scenario, the IoT SP needs to apply for the authorization of the security service from the IoT security service platform firstly, and then the SP can directly interact with the IoT device. Among them, legitimate IoT devices can encrypt business data and transmit them to the IoT SP through the security capabilities provided by the integrated SIM card. The SP verifies and decrypts the data through authorized verification; the SP platform can also send encrypted data to the Internet of Things terminal, thereby realizing end-to-end two-way secure data transmission. Due to the end-to-end encryption and integrity protection of data through IoT security services, eavesdroppers on the network cannot steal sensitive data.

In practical applications, for IoT SPs that use standard secure communication protocols (such as TLS, DTLS, etc.), IoT security services can provide security enhancement services for secure communication protocols. Security protocols such as TLS and DTLS can achieve end-to-end secure communication, but if you want to achieve terminal authentication, you need to preset a digital certificate and private key (or symmetric key) in the terminal, but once the key is stolen or there is potential risk will directly lead to the collapse of the entire security protocol. Therefore, the terminal needs a security mechanism to protect the private key, which undoubtedly poses a huge challenge to the IoT terminal.

The IoT security service based on SIM card can provide good support for the above requirements, that is, by storing the basic keys of security protocols such as DTLS in the SIM card and providing a key negotiation interface, thereby avoiding attacked risks of the security protocol basic keys, so as to achieve the security enhancement of the security protocol.

4.3.3. Local secure storage
The IoT terminal has some sensitive information, such as: PIN code, terminal identification and other information, and some terminal self-defined sensitive information. Some of these information are sensitive to reading, and some are sensitive to modification and need to be stored in a secure medium. The secure storage capability of the SIM card itself can just meet this demand. This is the local secure storage service. The SIM card provides secure storage services for IoT terminals through an open standard secure storage service interface and a certain amount of storage space.

A typical application scenario is shown in Figure 5:
Figure 5. Local secure storage

SP can write sensitive information into the SIM card of the IoT device safely after authorized by the security service platform, and then the APP on the IoT terminal can safely access the sensitive data in the SIM card locally. Attackers cannot obtain or tamper with these data. Thus, the protection of sensitive data in the terminal is realized.

4.4. Security Service Mode

4.4.1. Simple service model
Simple service mode is a simple and easy service mode. In this mode, the SP does not need to make major changes to its own SP platform. It only needs to integrate the SDK for accessing the SIM card on the terminal side, and implement a complete service process on the platform side through remote service calls to the security service platform. The solution is quick to access and low in implementation cost, as shown in Figure 6:

Figure 6. Simple service model

4.4.2. Self-service model
Self-service mode is a service mode that realizes SP's independent service. In other words, during the service process, the SP does not need to send a request to the security service platform, but only needs the SP service platform to process independently to complete the security service process, as shown in Figure 7:
Figure 7. Self-service model

The IoT SP needs to apply for authorization from the IoT security service platform first, and after obtaining the authorization, it has the ability to communicate securely with the SIM card. The subsequent communication, authentication, encryption and decryption operations between the SP and the IoT device can all be completed by the SP autonomously and independently.

5. Conclusions
With the rapid growth of the number of Internet of Things connections, the security needs of Internet of Things terminals are becoming more and more urgent. The current solutions are either low in security or high in cost. As the basic security medium on IoT terminals, the SIM card is the basic communication medium and can also provide various security services such as authentication, data secure transmission, local secure storage, etc. Therefore, the development of IoT security services based on the SIM card can make full use of this natural security carrier, which has good universality, high security, low cost, fast implementation, etc., and can become a preferred security solution in the field of Internet of Things.

References
[1] International Telecommunication Union. (2005) Internet Reports 2005: The Internet of Things. https://www.itu.int/pub/S-POL-IR.IT-2005/e
[2] IoT Security Innovation Lab. (2019) IoT Terminal Security White Paper. http://www.caict.ac.cn/kxyj/qwfb/bps/201911/t20191115_269625.htm
[3] Globalplatform. (2019) A practical implementation guide to secure IoT devices across all markets and in line with global requirements. https://globalplatform.org/resource-publication/ebook-introducing-iotopia/
[4] Globalplatform. (2014) The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market. https://globalplatform.org/resource-publication/the-trusted-execution-environment-delivering-enhanced-security-at-a-lower-cost-to-the-mobile-market/