Key Management Scheme Based on Micro-Certificate for Internet of Things

LiPing Du [12, a], FuWei Feng [12, b], JianWei Guo [12, c]

[1] Beijing Municipal Institute of Science & Technology Information, Beijing, 100044, China

[2] Beijing Key Laboratory of Network Cryptography Authentication, Beijing, 100044, China

[a]email: duliping_419@163.com, [b]email: feng_fuwei@126.com, [c]email: vipherovip@163.com

Keywords: Key Management; Micro-Certificate; IoT; CSK

Abstract. This paper presents a micro-certificate based key management scheme which mainly manage the keys relevant to the cryptography authentication system for internet of things (IoT), including key seeds, transmission key, storage key, authentication key and signature/encryption key. This paper gave detailed management scheme for keys' life cycle, and the combined symmetric key technology (CSK) and secure chip technology are used to improve the security for the key management in IoT environment.

Introduction

In recent year, the application of IoT become more and more widely. And the security of IoT is also very important [5], including the data collection security of sensor node, the information transmission security in the network and the security for business data processing etc. The key management is the base for all these security and is a mainly protection method to realize the authenticity, integrity and reliability for the information of the IoT [1]. In the internet environment, there is no limit of computing and storage etc resources. Both the asymmetric cryptosystem based on the PKI infrastructure and the symmetric cryptosystem can be applied well in the internet environment. But in the IoT, the public key protocol can't meet the security need because of the limitation of sensor nodes in the computing ability, storage space and power energy [6]. How to solve the key management problem include key assignment, update, storage and cancel, is the mainly task the IoT faced.

This paper presents the key management scheme based on the micro-certificate for IoT. The micro-certificate refers to the small certificate which is used in processing the security process to identify the sensor nodes device in the internet of things [2]. According to the special environment, the micro-certificate may be only a few bytes in size. Micro-certificate is based on the CPU security chip, and uses the symmetric cryptographic algorithms and CSK technology to realize the dynamic changes timely in the authentication, signature and encryption process. The micro-certificate has high security and fast speed, which can meet IoT environments well. The micro-certificate based key management scheme for IoT manage the relevant keys and provides the solid security foundation for the information security of IoT and ensure the confidentiality, authenticity, reliability and non-repudiation of information.

The Key Types

The Keys involved in the key management based on the micro-certificate are symmetric keys. That is the communication parties use the same key and encryption algorithm for data encryption and decryption. Symmetric key has the characteristics of short key length and low cost for computing and storage, which is very suitable for the IoT. The micro-certificate based key management includes following keys.

Key Seed

Key Seed [3] is key matrix of 61 rows and 16 columns K61×16]. It is generated by the hardware random number generator in the CPU smart chip. Each sensor device has a unique key seed. Key seed is stored in both the sensor side and authentication center. In the sensor end, the key seed is stored in CPU smart chip, and in the authentication center, the key seed is stored as cipher in the key database of authentication server. Key seed is as (1).

$$K_{61\times16} = \begin{bmatrix} Y_{5\times16} \\ M_{12\times16} \\ D_{31\times16} \\ R_{13\times16} \end{bmatrix} \tag{1}$$

In(1), $Y_{5\times16}$ is the sub key seed for year. In this scheme, 5 years key seeds are stored in the sensor nodes. $M_{12\times16}$ is sub key seed of month including 12 rows. $D_{31\times16}$ is 31 rows sub day key seeds, and $R_{13\times16}$ is the fix sub key seeds including 13 rows.

Transport Key

Transport key K_{trans} is used to protect the transmission of key seeds between the sensor nodes and authentication center. In the initial phrase, K_{trans} is fixed in the encrypt cards of authentication server and CPU smart chip of sensor nodes of IoT. K_{trans} is a symmetric key including 128 bytes.

Storage Key

Storage key K_{store} is to protect all the key seeds of senor nodes stored in the key database of authentication center. K_{store} is a 128 bytes symmetric key, and is fixed in the encryption cards of the same authentication server in the initial phrase. The storage key for different authentication server may be not the same. But for the encryption cards in same authentication server, the storage key must be the same.

Authentication Key

Authentication key K_{auth} is 128 bytes symmetric key generated from the key seed by using the CSK technology. In every authentication process, K_{auth} is used to encrypt the critical part of micro-certificate and form the authentication code for micro-certificate.

Signature/Encryption Key

Signature/encryption key K_{sign} is also the 128 byte symmetric key generated from the key seed by using the CSK technology. In every digital signature process, K_{sign} is used to encrypt the data digest and form the signature for the micro-certificate. At the same time, signature/encryption key is used to encrypt the plaintext in the more secure application.

Key Life Cycle

Each key has its own life cycle, and the key management is to manage the key life cycle. The life cycle includes the key generation, key distribution, key execution and key revocation etc processes. The micro-certificate based key management system manages keys as the table 1 [4].

TABLE I. KEY TYPE AND LIFE CYCLE

Type Life Cycle	Key-seed	Transport key	Storage key	Authentication key	Signature/Encryption Key
create	Hardware random number generator	Hardware random number generator	Hardware random number generator	CSK algorithm	CSK algorithms
storage	Smart chip/key database	smart chip/encrypt card	Encrypt card	One-time one-variant	One-time one-variant
distribution	Encrypted by the transport key	Physical isolation	Physical isolation	\	\
update	5 years	\	\	Real time	Real time
revocation	Key management system	\	\	Real time	Real time

Management of Key Seed

1) Generation of key seed: Key Seed is generated by the hardware random number generator in the smart card chip of sensor nodes. It is a set of hexadecimal random code. The key seeds in each sensor secure chip are different from each other. Each key seed is generated independently and stored in its own corresponding secure chip. The security storage of key seed is realized.

2) Distribution of key seed: In order to realize the secure distribution, key seed is transferred to authentication center by cipher. Then the cipher of key seed is stored in the key database of authentication server, and the transport security and storage security are ensured. The small-scale sensor devices' key seeds can be distributed as Fig.1. The large-scale sensor devices' key seeds distribution needs the third party to write data centralized.

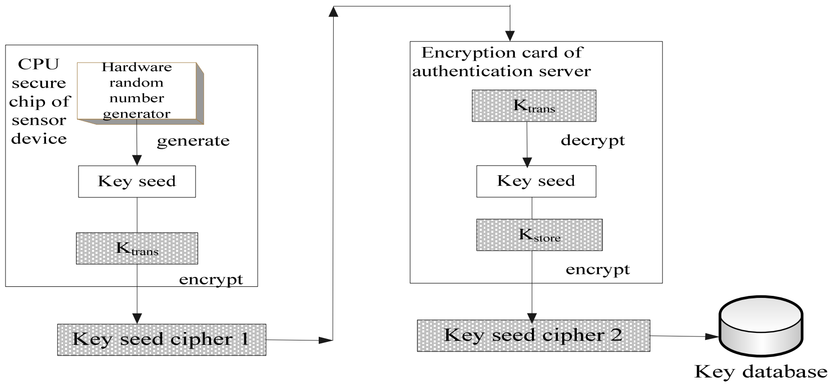

Fig.1 key seed generation and distribution

3)Key seed update: Key Seed is the key pool to generate the keys. Each key seed of sensor node is about 1K bytes, and the year sub key seed is a matrix of 5 rows and 16 columns $Y_{5\times16}$. Key seed can be updated every 5 years. The update can be remotely operation from the authentication server to download the update command.

4) Revocation of Key Seed: The revocation operation can be executed in the key manage system. Namely, the key seed in the CPU secure chip is invalid. This operation can also be executed remotely.

Management of Transport Key

1) Generation of transport key: Transport key is generated in the key initialize phrase. First, a set of 128 bytes random number is generated by the hardware random number generator in the encryption card of authentication server. The 128 bytes random number is as the transport key K_{trans}. K_{trans} is stored in both the encryption cards of authentication centre and CPU secure chip of sensor node. K_{trans} in the encryption cards of authentication centre must be the same. K_{trans} is to ensure the security of key seed transport between the sensor node and authentication centre.2) Distribution of transport key: In the initial phrase of key, K_{trans} is generated by the encryption card of authentication centre and then K_{trans} is distributed to all smart chips of sensor nodes. Transport key mainly protects the secure transport of key seed. The generation and distribution of transport key is done in off line, that is, the process environment is local subnet and is isolated from the internet which can guarantee the security for transport key generation and distribution.3) Execution of transport key: K_{trans} is mainly used to ensure the secure distribution of key seeds. When the key seeds are distributed to each sensor node, they are first encrypted by the transport key K_{trans}. After that, the encrypted key seeds are transported to the authentication center securely.4) Update and revocation of transport key: K_{trans} is stored in the hardware chip, and is only used in the initialization of key, so the update and revocation of transport key is not needed.

Management of Storage Key

The storage key K_{store} is used to encrypt the key seeds of all the sensor nodes in the authentication center and to protect the security of key seeds.

1) Generation of storage key: K_{store} is generated by the hardware random number generator in the encryption card of authentication center. It is a set of random numbers which has 128 bytes long. K_{store} is mainly used to protect the security of key seeds for all the sensor nodes in the IoT. The

generation and distribution of K_{store} are processed in the local network and is isolated from internet.2) Distribution of storage key: K_{store} is stored in more than one encryption cards, and is distributed by the main encryption card to other encryption cards in the authentication server. The K_{store} for different authentication servers may be same and may be different. But in a authentication server, K_{store} in each encrypt card must be the same.3) Execution of storage key: When the authentication serve receives the key seeds from the sensor nodes in IoT, the encrypt card of authentication centre call the K_{trans} of CPU chip to decrypt the key seeds. Then the K_{stroe} is called to encrypt the key seeds to get key seeds cipher. Key seeds cipher is stored into the key database. The security storage of key seed in the authentication center is realized.

Management of Authentication Key

Each time the sensor node begins a authentication request, the authentication protocol will call the CSK algorithm to select and combine elements form the key seeds in the smart chip according to the time stamp and random number to generate the authentication key K_{auth}. K_{auth} is generated in the smart chip of sensor nodes. K_{auth} is used to encrypt the critical part of micro-certificate. The update rate for K_{auth} is $1/2^{64}$, which almost changed each time, and is not reused. The revocation of K_{auth} is real time too. When the authentication process is finished, K_{store} is invalid.

Management of Signature/Encryption Key

When the sensor nodes in IoT request data signature operation, the signature protocol will call the CSK algorithm to select the elements from the key seeds of smart chip according to the time stamp and random number control parameters to form the signature/encryption key K_{sign}. K_{sign} is generated in the smart chip of sensor nodes. K_{sign} is used to encrypt the digest and create the signature of micro-certificate. K_{sign} changed each time and the update rate is 1/264. When the signature process is finished, K_{sign} is invalid.

Key Back Up and Disaster Recovery

In order to prevent the key seeds information being stolen or tampered with, the micro-certificate based key management system provides the tamper-resistant function for important data. Through computing the digest for key seeds in database timely, and comparing the digest result with the one in encrypt card to ensure the key seeds information not being tampered with. So the key management system of IoT can run normally.

When key seeds is initialized or updated, the system will start the key back-up and disaster recovery function, and the digest of key seeds will be stored in the encrypt card, which can ensure the system verify the new and complete data. The system will also back up key seeds timely. If the tampering or other abnormal conditions are detected, the system will recover the key database according to the back-up data. So the micro-certificate based security system of IoT can be ensured to be safe and credible.

The Critical Technology

Adoption of CSK Technology

CSK technology [7] uses the time stamp and random number as the control parameters. In each authentication or signature/encryption request, CSK algorithm is call to generate the authentication key or signature/encryption key through selection and combination from the key seeds. And the micro-certificate for authentication or signature is generated.

Key's Randomness and Credbility

Hardware random number generator ensures the random number generated has the randomness and unpredictability, which meets the cryptography security standards. So key seeds for each sensor nodes of IoT have the randomness and unpredictability, and the control parameters random number which are used in the security protocol including authentication, signature and encryption are also randomness and unpredictability. Therefore the security keys including authentication key and signature/encryption key are changed each time, which protect the security of cryptography system of IoT effectively.

Security Storage of Key

1) Key seeds generated by the hardware random number generator are stored in the CPU smart

chip of sensor nodes. In authentication center, key seeds are stored in the key database as cipher. Both in sensor nodes and authentication server, hackers can't get or tamper with the key seeds illegally.2) Transport key and storage key are also stored in the hardware chip, and the distributions of both keys are in a isolated network environment, which prevent the disclosure of keys.3) The authentication key and signature/encryption key are dynamic generated and cancelled. Their life cycle is in the memory. In some sense, they are stored securely.

Conclusions

This paper proposed a key management scheme based on micro-certificate for IoT. This scheme mainly provides service for cryptography authentication system of IoT. In the key management based on micro-certificate, the keys involved include key seeds, transport key, storage key, authentication key and signature/encryption key. This paper introduces the generation, distribution, storage, update and revocation for all these keys in detail. At the same time, the critical technologies which are used to protect these keys are also introduced. Keys in micro-certificate based key management scheme are all symmetric keys which mean that they occupy small space and have fast encryption/decryption speed [8]. The micro-certificate based key management scheme is very suitable for the large-scale application system of IoT, and can provide the high security performance for IoT.

Acknowledgment

This work was financially supported by Program of Large-scale Network Authentication Center affiliated to Beijing Municipal Institute of Science & Technology Information (No. PXM2012_178214_000005).

References

[1] G. Yang, J. Xu, Wei Chen, Z.H. Qi, H.Y. Wang “Security Characteristic and Technology in the Internet of Things,” Journal of nanjing university of posts and telecommunications(natural sciemce), vol. 30 (4) ,2010.

[2] L.P. Du, Y. Li, G.N. Xu, F. Duan, “Research on Micro-Certificate based Security System for Internet of Things,” Applied mechanics and materials Vols.263-266, 2013, pp.3125–3129.

[3] .Y. Hu, G.F. Zhao, “A CSK-based Solution for Person Authentication,” the Seventh wuhan international conference on e-business: unlocking the full potential of global technology. 2008, pp.244-249.

[4] L.P. Du, J.W. Guo, Y. Li, “Research on Micro-Certificate based Authentication Protocol,” Proceedings of the 2nd international conference on computer science and electronics engineering, 2013, pp. 0443-0446.

[5] L. Guo, B. Yan, Y. Shen, “Study on Secure System Architecture of IOT”, China infromation security, vol.12, 2010, pp73-75.

[6] Z. Su, C. Lin, F.J. Feng, F.Y. Ren, “Key Management Schemes and Protocols for Wireless Sensor Networks,” Journal of software, Vol. 18, No.5,May 2007, pp.1218-1231.

[7] L.P. Du, Y. Li, G.F. Zhao, “The Design and Implementation of Accelerated Authentication System for Mobile Platform”, 2010 International conference on information, networkong and automation, 2010,pp.V1-503-V1-506.

[8] B. Schneier, “Applied Cryptography”, Wu Shizhong, Zhu Shixiong, Zhang Wenzheng. Beijing: China Machine Press. 2000.