Discussion on the Integration of Common Key Management and Internet of Things

Gege Tian

School of Software, Zhengzhou University, 450002

Keywords: IoT; Information security; Key Management

Abstract: The Internet of Things (IoT) completes the direct integration of computing systems with the physical world .It reduces costs for manual, and it improves efficiency while facilitating people's lives, and brings enormous economic benefits. However, with the increasingly deep integration of the Internet of Things with people's production and life, some characteristics of the Internet of Things itself also pose a huge threat to security and privacy. Cryptographic technology is the core of information security, and the key is the basis to ensure the security of cryptographic technology. Therefore, it is very important to establish a suitable and perfect key management system in the environment of the Internet of Things. Starting from the characteristics of the Internet of Things, this paper analyses the requirements of these characteristics for key management. The three main key management systems in the Internet environment, Public Key Infrastructure, Combined Public Key and Identity-based Cryptograph, are introduced and discussed. The advantages and disadvantages of these key management systems in the Internet of Things environment are discussed and compared from three aspects.

1. Introduction

The development of the Internet of Things is very rapid. Politicians as well as practitioners estimates currently suggest that the IoT could grow into a market worth $7.1 trillion by 2020 (IDC 2014).[3] At the same time, its popularity and deep integration in various application scenarios also pushed the world into a new era of interconnection. The Internet of Things (IoT) is fully aware, reliable and intelligently processed, which brings great convenience and comfort to production and life. However, due to its deep integration with production and life, it also brings risks of security and information disclosure.

Cryptographic technology is the core of information security, and the key is the basis to ensure the security of cryptographic technology. Compared with traditional communication networks, in the Internet of Things environment, there are a large number of terminals with limited computing and storage capabilities, and some terminals have the requirements of direct and offline authentication[8]. Therefore, selecting an appropriate key management system and management mechanism for the characteristics of the Internet of Things is an important content to ensure the information security of the Internet of Things.

2. Features of Internet of Things Terminals

2.1 Large number of terminals and diverse forms

"Connectivity of all things" is a pursuit of the Internet of Things, which also causes the number of terminals in the Internet of Things to increase geometrically in magnitude, and the diversity of access system terminals also complicates the authentication relationship. In the face of such a complex terminal device, the necessity and difficulty of key management will increase dramatically.

2.2 Terminal's own resources are limited

In the Internet of Things environment, terminal nodes are mostly devices based on small embedded systems, and their computing and storage resources are limited. The computational and

storage resources required for authentication between devices should not be too high. To coordinate security and resource constraints, make the key system as lightweight as possible.

2.3 Requirements for direct and offline authentication between terminals

Due to the bandwidth limitations of the Internet of Things itself and the application scenarios, there will be scenarios between terminals that require direct and offline authentication. It is worth considering that real-time performance is maintained with limited bandwidth and that authentication can be as reliable as possible while offline.

3. Key Management System Overview

In the current Internet key management system, the major key management schemes that can be applied to a large scale are Public Key Infrastructure (PKI), Combined Public Key Cryptosystem, identity-based cryptograph (IBC).These three systems are described below.

3.1 Public Key Infrastructure

PKI is currently the most used key management system in the Internet. The core of PKI is certificate authority (CA).The CA acts as a trusted third party to guarantee the identity of each principal in the system and the legality of the public key. After the principal's key and identity information are signed by the CA, the generated certificate [6] is stored in the public directory for retrieval and used to implement functions such as encrypted signature, identity authentication and so on.In providing services, the CA must provide the CA's own public key to its authenticated principals and trusted principals who may use the authentication information, and use a hierarchy as needed. The authenticity of the public key of a subordinate CA is guaranteed by a superior CA. The structure of the PKI is illustrated below.

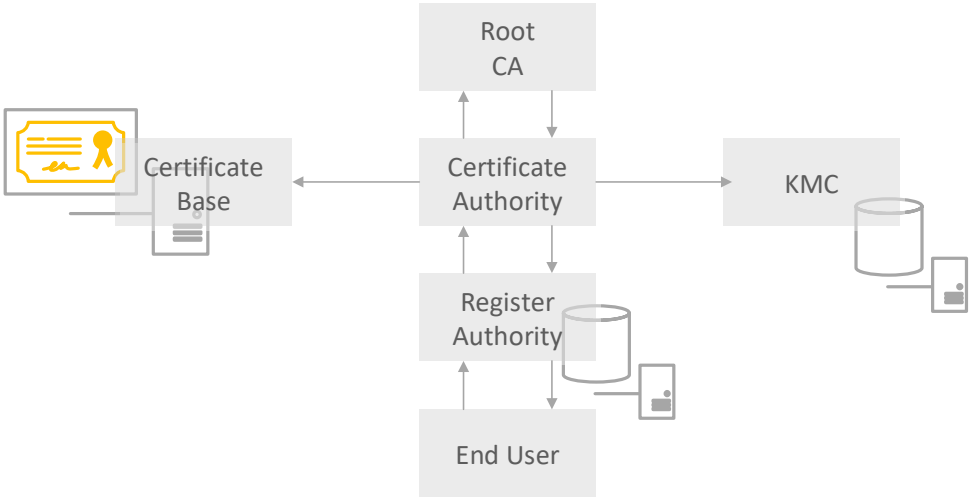

Fig.1

3.2 Combined Public Key Cryptosystem

The combined public key (CPK)[9][10] was first proposed by Professor Nan Xianghao of China. CPK is based on Elliptic Curve Cryptography (ECC), which uses a small number of "seeds" in the matrix to generate a large number of public keys.

Choosing a resistant group of elliptic curves E / F_p and elliptic curves based on a finite domain. Suppose the base point is G and its order is prime n.Assuming the private key sk is any integer r, the corresponding public key pk is a point rG on elliptic curve E marked with (x_r, y_r).[1]

The private key seed matrix SSK is made up of integer vector PSK while the public key seed matrix PSK is made up of the corresponding point vector $(r_{ij}G) = (x_{ij}, y_{ij})$.[1]

$$SSK = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1h} \\ r_{21} & r_{22} & \cdots & r_{1h} \\ r_{21} & r_{22} & \cdots & r_{2h} \\ \vdots & \vdots & & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mh} \end{pmatrix}$$

$$PSK = \begin{pmatrix} (x_{11}, y_{11} & (x_{12}, y_{12}) & \cdots & (x_{1h}, y_{1h}) \\ (x_{21}, y_{21} & (x_{22}, y_{22}) & \cdots & (x_{2h}, y_{2h}) \\ \vdots & \vdots & & \vdots \\ (x_{m1}, y_{m1}) & (x_{m2}, y_{m2}) & \cdots & (x_{mh}, y_{mh}) \end{pmatrix}$$

The seed matrix is produced offline by the trusted third party Key Management Center (KMC), the private key seed matrix is kept secret, and the public key seed matrix can be published and distributed to the principal.[1]The center chooses the one-way trap function as the query function appropriately (PSK and SK use the same selection method), uniquely determines a combination of column factors based on the unique identity information of the principal, and sums up the public key and private key of the principal, respectively. The principal can directly use the query function to complete the offline query in the PSK, which is equivalent to obtaining all the public keys at once.

3.3 Identity-based Cryptograph

Identity-based cryptography (IBC) was introduced by Shamir[5]. The main idea of IBC is to take the user's identity information as the public key directly, so as to avoid identity authentication and public key management. IBC has only one private key generator (PKG), which is responsible for producing global parameters and calculating the private key of the principal. At the same time, the security of the whole system only depends on the secrecy of the PKG private key. Some mapping functions are frequently used in key generation of IBC, which results in a large amount of computation. For various reasons, IBC is not widely used.

4. Discussion and Comparison of Three Key Management Systems in the Environment of Internet of Things

4.1 Analyzing from Key Storage

In the PKI system, a principal corresponds to a certificate. In the context of the Internet of Things, a large number of device certificates will bring inconvenience to storage and maintenance. Once the CA's capability is insufficient, the level of PKI needs to continue to expand, which leads to the risk of certificate reliability and the improvement of authentication barriers.

In CPK, only one matrix is needed to complete the storage of a large number of public keys, which is small, convenient to save and has obvious advantages in the Internet of Things environment.

In IBC, the center only needs to save its own private key, because it can be exported as a user in IBC. However, this also poses a huge security risk, because if the private key of the center is compromised, the system will crash.

4.2 Analysis from Key Management

CA in PKI is dynamic in certificate management, large in maintenance and high in cost, but its key exchange is more convenient.

In CPK, the principal establishes the authentication relationship at the time of registration, and subsequent maintenance only needs to establish a blacklist to update regularly. However, there is

also an inconvenient problem to change the key in CPK[7]. At this time, variable factors can be introduced into the system to use multi-factor combination of public keys to solve the problem of key exchange flexibility.

4.3 Analyzing from Certification Function

In the PKI system, when key negotiation and certification are carried out, digital certificates need to be exchanged. The authenticity verification of digital certificates by both sides depends on CA for online verification. At the same time, if there are more CA levels, it may also need one level to complete authentication, which poses a high challenge to the bandwidth of the Internet of Things communication network.

In CPK, the public and private keys of CPK are generated by KGC, which corresponds to its identity and has high reliability in authentication. When both parties authenticate, they only need to query the public key matrix locally to verify the identity of the other party, which makes offline authentication possible. It is faster, more reliable and requires less bandwidth.

In IBC, the identity is the public key, that is, there is no need to authenticate, because IBC is the authentication of KGC. Therefore, IBC consumes less bandwidth on the network during authentication in the Internet of Things environment.

5. Conclusions

The rapid development of the Internet of Things cannot be separated from the protection of information security. Cryptography technology is the core of information security, and the key is the basis to ensure the security of cryptography technology. Therefore, it can be seen that only by establishing a dedicated and perfect key management system can we meet the various challenges in the development of the Internet of Things. In this paper, the advantages and disadvantages of three major key management systems in the Internet environment are analyzed. PKI management is transparent and scalable, but it is difficult to meet the characteristics of large number of terminals and offline authentication in the Internet of Things. CPK is more efficient and economical. Its large amount of key storage space has strong advantages for the management of mass key storage in the Internet of Things, but there are some difficulties in key replacement. IBC is low-cost, scalable, and does not require key management and authentication, but its security remains controversial. It can be seen that these management systems are not perfect in such a special application scenario as the Internet of Things. How to transform and mix them for the application scenario of the Internet of Things needs us to continue to conduct in-depth research.

References

[1] Ji Jiafa Z, Tao M, Yifa L. Comparison and Analysis of PKI, CPK and IBC [J]. Journal of Information Engineering University, 2005, 6(3): P26-31.

[2] Zhi-guang Z B Q I N, Guo-gen W A N. Study on Hybrid Key Management Mechanisms of RFID System Based on PKI and CPK [J]. Journal of University of Electronic Science and Technology of China, 2015, 44(3): 415-421.

[3] Wortmann F, Flüchter K. Internet of things [J]. Business & Information Systems Engineering, 2015, 57(3): 221-224.

[4] Das A K, Zeadally S, He D. Taxonomy and analysis of security protocols for Internet of Things [J]. Future Generation Computer Systems, 2018, 89: 110-125.

[5] Guo H, Zhang X, Mu Y, et al. An efficient certificateless encryption scheme in the standard model[C]//2009 Third International Conference on Network and System Security. IEEE, 2009: 302-309

[6] Hunt R. Technological infrastructure for PKI and digital certification [J]. Computer communications, 2001, 24(14): 1460-1471.

[7] Yuguang H. Technical characteristics and application of CPK certification system [J]. Electronic Science and Technology Review, 2005, 2(17): 5-10.

[8] SARMA A, GIRAO J. Identities in the future internet of things [J]. Wireless Peers Communication, 2009,49(3):353-363.

[9] WANG Jia-lin. Comparative analysis of large scale etwork authentication scheme based on CPK and PKI[J]. Security Science and Technology, 2012(6): 44-46.

[10] NAN Xiang-hao. CPK algorithm and identity authentication [J]. Information Security and Communications Privacy, 2006(9): 51-54.