Research on Micro-Certificate based Authentication Protocol

LiPing Du
Beijing Municipal Institute of Science & Technology
Beijing Key Laboratory of Network Cryptography
Beijing, China
duliping_419@163.com

JianWei Guo Ying Li
Beijing Municipal Institute of Science & Technology
Beijing Key Laboratory of Network Cryptography
Beijing, China
vipherovip@163.com shai_wang@hotmail.com

***Abstract*—This paper presents a micro-certificate based authentication protocol, which is lightweight and can be used in the internet and in the internet of things. The micro-certificate is a small, and is a dynamic certificate that changed each time and can improve the security of authentication protocol. The micro-certificate based authentication protocol uses the symmetric cryptographic algorithms, CSK technology and chip technology to improve the speed and security performance for the authentication process.**

Keywords-micro-certificate; authentication; combined symmetric key; chip; protocol

I. INTRODUCTION

The identity authentication technology is a critical technology to realize the information security. No matter in the internet environment or in the things of internet environment, the identity authentication is the first barrier of the whole security platform. Once the authentication system is broken, the all other security mechanisms will exists in name only [10].

The current identity authentication mechanism includes the password based authentication, PKI/CA digital certificate and biometric authentication mechanisms. The password based authentication is simple and easily deciphered [5]. The PKI/CA digital certificate is widely used, but the large certificate and complex certificate chain based authentication process and the vulnerable root certificate, all these limit the PKI/C's development [7, 8]. Especially in the internet of things, because of the sensor nodes has the characters of small storage space and low processing capacity, PKI/CA is not in its place. The biometric based authentication mechanism has the security and reliability [6] which the other authentication techniques are unable to compare with. However, due to the high cost of identification equipment and unstable characteristic factor, the biometric based authentication mechanism can't be widely used, especially in the internet of things [10], it is not suitable.

Based on the above consideration, this paper presents a micro-certificate based authentication protocol. This authentication mechanism uses the less authentication parameters to form the micro-certificate for the authentication protocol, and CPU security chip is used to store the important secret information. At the same time, the micro-certificate uses the symmetric cryptographic algorithms to realize the authentication process which leads to the high security and fast speed. The micro-certificate based authentication protocol can be applied both to the internet and the internet of things environment.

II. MICRO-CERTIFICATE

A. Defination for Micro-Certificate

The micro-certificate refers to the small certificate which is used in processing the authentication process to identify the user or the terminal device in the internet of things. 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 process. The micro-certificate has high security and fast speed, which can meet various network environments. The main features of micro-certificate are as follows

- Small storage. The most important feature of the sensor device in the internet of things is weak processing power, small storage space, which inevitably need the primary characteristics of micro-certificate to occupy less space resources. In this security system, the micro-certificate is composed of dozens of bytes, and the micro-certificate based lightweight authentication can be achieved.
- Fast speed. During the process of authentication, the micro-certificate uses the symmetric cipher mechanism, and compared with the asymmetric algorithms, the most important feature of the symmetric cryptographic algorithm is fast speed and high performance.
- High security performance. The high security is mainly reflected in the following two aspects: First, The chip-level security protocols are used. The authentication protocols are running in the chip and protected by the chip hardware. Second, the composed symmetric key (CSK) [1, 2] is used to realize the micro-certificate one-time-one-variant, and improve the security of micro-certificate.

B. Key Management for Micro-Certificate

The generation of micro-certificate involves strict key management process. In the micro-certificate based authentication protocol, the following key concept is mainly involved:

- Key-base: a key matrix. It is a group of random number generated by the hardware random generator.

Published by Atlantis Press, Paris, France.
© the authors

Each user's (or device's) key-base is stored in his own CPU security chip, and are different from each other. All users' key-bases are stored in the server as cipher.

- Transmission security key: is used to protect the key-base transmission between the client and authentication center. It is initialized in the initial phrase of system, and is fixed in the CPU security chip both in the client end and the authentication center.
- Storage key: is used to protect all clients' key-base stored in the authentication center. The storage key is fixed in the encrypt card in the initial phrase of the authentication system.
- Authentication key: is generated in the key-base through the CSK technology. In each authentication process, the important part of micro-certificate is encrypted by the authentication key, and the authentication key is also used to encrypt the authentication code as the symmetric key.

The key class and management of micro-certificate are shown as table 1.

TABLE I. KEY CLASS AND MANAGEMENT OF MICRO-CERTIFICATE

Class / Management	Key-base	Transport key	Storage key	Authentication key
generation	Hardware random number generator	Hardware random number generator	Hardware random number generator	CSK technology
storage	Security chip/authentication center data base	Security chip/encrypt card	Encrypt card	Changed each time, not need storage
distribution	Encrypted by the transport key	Physical isolation	Physical isolation	\
update	***10*** years	\	\	Changed each time
Cancellation	Key management system	\	\	\

C. *Format of Micro-Certificate*

The micro-certificate includes the following content mainly:

- Message head: used to identify the function of micro-certificate. When the authentication center receives the micro-certificate, it will perform the corresponding authentication process based on the message head.
- User (device) ID: used to identify the user in the network or the terminal device in the internet of things uniquely.
- Time-stamp: the time of authentication. According to the special application needs, the time-stamp can be sent to the client by the server, or can be created at the client directly. The time-stamp is accurate to seconds.
- Random number: is generated by the hardware random number generator. Random number and time-stamp are both as the control parameter to create the micro-certificate.
- Authentication code: is secret data of micro-certificate, generated based on the authentication key and symmetric cryptographic algorithms. Authentication code is composed of 16 bytes, and is a variable code dependent on the random number and timestamp.

The specific format of micro-certificate is followed as table 2.

TABLE II. THE FORMAT OF MICRO AUTHENTICATION CERTIFICATE

Message Head	Sensor ID	Time stamp	Random number	Authentication code
1 byte	4bytes	7bytes	8bytes	16bytes

III. THE AUTHENTICATION PROTOCOL BASED ON THE MICRO-CERTIFICATE

At the client end, the CPU security chip is deployed. In the internet environment, the client user can have the USB key and in the internet of things, the sensor terminal can be equipped with cipher chip according. At server end, the encrypt card or cipher machine is set up. In the process of authentication, the client generates the micro-certificate through calling the micro-certificate generation protocol in the CPU security chip at first. Then the client submits the micro-certificate generated this time to server to verity its identity.

A. *Micro-Certificate Generation Protocol*

Micro-certificate is generated dynamic in each authentication process, and becomes invalid at the end of authentication. It is a dynamic certificate which changes each time. Under the effect of the dual control parameters of time stamp and random number, the security module at the client will call the CSK algorithms [1,2] in the CPU security chip to perform computation in key-base, and generate authentication key which is used in this authentication process. Then the authentication code is created by the authentication key and symmetric cryptographic algorithms. Finally, the security module composed the time-stamp, random number and authentication code to generate the micro-certificate.

© the authors

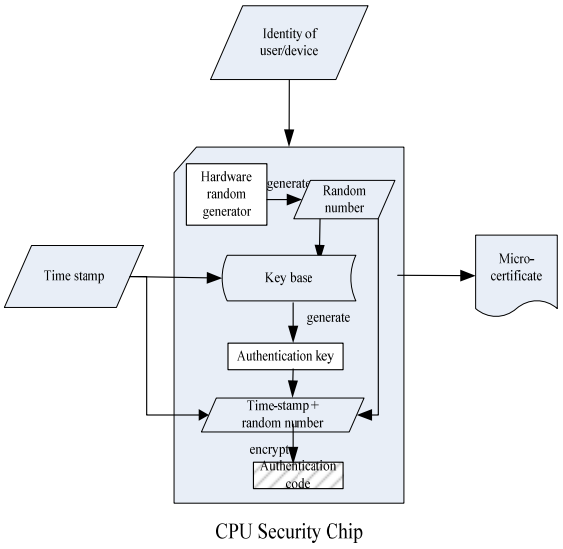

Figure 1. The micro-certificate generation protocol

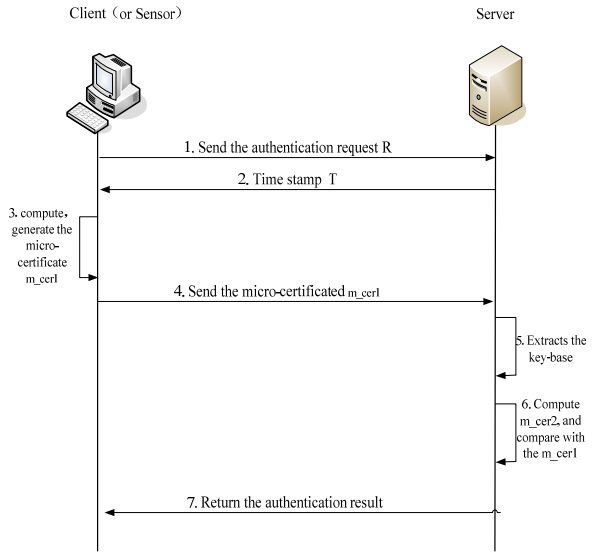

Figure 2. The micro-certificate based authentication protocol

Micro-certificate generation protocol is a dynamic security protocol, and its repeat probability is $/12^{64}$ a minute. The one-time-one-variant characteristic of micro-certificate provides the advanced security for the authentication process. Also, micro-certificate protocol is a chip-based protocol; all relevant key operation is performed in the CPU security chip, which also ensures the authentication security.

B. The Micro-Certificate based Authentication Protocol

- The client submits the authentication requests to the server.
- The server generate a time stamp T, and sends the time stamp T to the client as a challenge
- The client receives the time stamp, and generates the micro-certificate m_cer1 using the micro-certificate generation protocol.
- The m_cer1 is sent to the server. At this point, the micro-certificate not only as the certificate to identify the client identity uniquely, but also as a response parameter sent to the server.
- The server must determine the T in the m_cer1 is correct, and then extracts the corresponding the key-base according to the user/device ID in the micro-certificate.
- The server sends the time stamp, random number and key-base which extracts from the micro-certificate to the encrypt card. The copy of micro-certificate m_cer2 is generated. Through comparing the m_cer1 with m_cer2, the server can determine the client identity.
- The server returns the authentication result, and the authentication protocol based on the micro-certificate is finished.

The authentication protocol is shown as Figure 2.

In the micro-certificate based authentication protocol, the challenge-response mechanism is used to prevent replay attacks. In the response parameter m_cer1, the time-stamp generated from the server is also included. So the server will first check the time-stamp to judge if the micro-certificate is replayed.

All users' key-bases are stored in the server database as cipher. During the generation of micro-certificate copy m_cer2, the corresponding key-base's decryption operation and other key operations are performed in encrypt card and ensured the security.

IV. ANALYSIS OF PERFORMANCE

A. Security Analysis

The micro-certificate based authentication protocol has the high security, which is shown as following two points:

1) The Chip Based Secuirty: Both in the client and server, the cryptographic hardware is used. The CPU security chip or USBKey is deployed in the client, and the server is equipped with the encrypt card. So the chip based channel is built. Furthmore, the cryptographic hardware meets the secuirty standards of the State Cryptography Administration. All the key operations related to micro-certificate are performed in the secuirty chip. So the secuirty is ensured from the hardware point of view, preventing secret information being stolen by hackers.

2) The dyanmic characteristics: The micro-certificate is dynamic certificate which means it changed in each authenticaion process. The time-stamp and random number wich used to generate the micro-certificate determine the dynamic characteristics. The repeat probability of the micro-certificate can reach to $1/2^{64}$ times each minute. So that even if the micro-certificate is intercepted by the hacker during the transimission, the security is not affected, and the replay attacks are prevented.

© the authors

The dyanmic characristics of micro-certificate depends on the authentication code. The authentication code is a 16 bytes variable. Each byte is selected from 16 bytes sub key-base.So the repeat probability of micro-certificate MP is computed as follows:

$$MP = (16)^{16} = 2^{64} \quad (1)$$

B. Speed Analysis

The micro-certificate based authentication protocol has the quality of fast speed.

1) The CSK technology is used: The micro-certificate based security system uses the symmetric cryptographic algorithms which has more fast computation speed. Compared with the mainly used asymmetric cryptographic algorithms, the symmetric cryptographic algorithms greatly improve the authentication speed efficiency[4]. Simultaneously, this system uses the CSK technology to solve the problem of symmetric key distribution and greatly reduce the costs of key update and maintenance.[3]

2) The micro-certificate is small: The small size is a very large advantages in the authentication process. At first, the less bandwith is used during the transimission. Second, on the server side, when the certificates are compared to determine the client identity, because of the micro-certificate is based on the ID feature, the retrieval speed of micro-certificate is increased. Especially in the internet of things enviroment, the micro-certificate can play more important role because of the shortage of resource-constrained of the sensor nodes.

V. CONCLUSIONS

This paper proposed a micro-certificate based authentication protocol. The micro-certificate mainly uses the symmetric cryptographic algorithms, CSK technology and cipher chip technology to realize the authentication. Compared with the other authentication protocol, the micro-certificate protocol has the advantage of small size, fast speed and high security. After the tests by assessment center, the concurrent capacity of authentication for the micro-certificate based security system is up to 1000 times/1second. The micro-certificate based authentication protocol not only meets the large-scale authentication of network, but also applies to the authentication of sensor devices in internet of things.

ACKNOWLEDGMENT

This work was financially supported by Program of Network Authentication Lab affiliated to Beijing Municipal Institute of Science & Technology Information (No. PXM2011_178214_000007).

REFERENCES

[1] Xiangyi Hu, Guifen 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.

[2] LiPing Du, Ying Li, GuiFen 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.

[3] Bruce Schneier, Applied Cryptography, Wu Shizhong, Zhu Shixiong, Zhang Wenzheng. Beijing: China Machine Press. 2000.

[4] K.J Zhou, X.L. Zuo, “Network Data Security System Based on Des and RSA”, Computer Engineering and Applications, North China Computing Technology Institute, 1998.9, pp.12-13.

[5] JingKu Li, DeYun Zhang, Yong Zhang, “Research of User Authentication Mechamnism and Its Security Analysis”, Application research of computers, 2001,18(2).

[6] YuangPing Xiang, ZiNan Ning, “Design and Implement of Authentication System based on Face Recognition Dual Factors”, Computer measurement & Control, 2009,17(5).

[7] ZhiGui Liu, LiChun Yang, Jie Pu, Shuang Zhang,”The System of Digital Signature Authentication Based on PKI”, Application Research of Computer, 2004, 21(9).

[8] Ying Sha, Shuo Bai, “On the Research and Analysis of the Main Problem of PKI”,Micro Electronics and Computer,2002,19(6).

[9] Xian Yu, Yu Long, XianPing Mao, “Research on TPM-based Strong ID Authentication protocol”, Computer Engineering, 2012, 38(4).

[10] Chen Yu, Wang JinDong, “Study on Authentication Protocols for Wireless Senso Network”, NetInfo Security, 2011,(12)

© the authors