Open Journal of Social Sciences, 2016, 4, 59-63
Published Online July 2016 in SciRes. http://www.scirp.org/journal/jss
http://dx.doi.org/10.4236/jss.2016.47009

Building a Secure Mobile Payment Protocol in the Cloud

Liping Du, Guifen Zhao, Ying Li

Beijing Municipal Institute of Science & Technology Information, Beijing, China
Email: duliping_419@163.com

Received 2 June 2016; accepted 18 July 2016; published 25 July 2016

Abstract

This paper is mainly to resolve the secure problems of mobile payment business which the remote payment is their main businesses. The identity authenticity of mobile payment user, the confidentiality and non repudiation of information transmitted in the mobile payment process are all the main secure problems. The secure mobile payment protocol is established base all the above secure problems' solutions.

Keywords

Secure UIM, Mobile, Payment, Protocol

1. Introduction

With the continuous development of 3G and 4G technology, the China's mobile internet rise rapidly. Mobile internet era subvert the desktop internet era of human production and life method, and create a new mode of information dissemination and business model. Until June 2015, the size of China's mobile phone users reached 594 million, increased 36.79 million compared with the people in 2014 [1]. The proportion of the mobile phone users is 88.9%, increased 3.1 percentage points compared with the end of 2014. The status that the mobile phone is the first major internet terminal equipment is more consolidate. "China Mobile Payment Market Research Report 2014" released by Analysis tank mentioned that Chinese mobile payment market in 2013 entered the explosive growth stage, the overall trading size exceeded 1.301 trillion yuan, the chain relative ratio increased 800.3% compared with the 2012. From the third quarter of 2013 to the first quarter of 2014, mobile payment transactions grew by more than 100%. Mobile payment users reached 125 millions, the year on year growth is 126.0%. This fully shows that the era of mobile payment has come. However, in this high-speed development, the security problem of mobile payment also deserves our concern. The latest reports from several major domestic internet security giant display that the mobile phone virus especially the virus of mobile payment growth exponentially, and the means hackers used to steal money and personal information are more subtle. Once famous "Prism" incident also prompts us to focus on information security issues of mobile payment.

Security problems of mobile payment services mainly related to the authenticity and validity of identity of the transaction parties, which is the basic conditions for e-commerce. The confidentiality of transaction data prevents malicious users to intercept or peek information. The integrity of transactions data ensures non authorized users can not change the transaction information. And the non-repudiation of transactions prevents the transac-

How to cite this paper: Du, L.P., Zhao, G.F. and Li, Y. (2016) Building a Secure Mobile Payment Protocol in the Cloud. *Open Journal of Social Sciences*, **4**, 59-63. http://dx.doi.org/10.4236/jss.2016.47009

tion parties deny their behavior after the transactions. The main security mechanism used in the current field of mobile payment is WPKI mechanism. WPKI, the wireless public key infrastructure, is a extension of traditional public key infrastructure in a wireless network environment. Although WPKI has a number of optimizations on the encryption algorithms and certificate format with respect to the PKI mechanism [2], but it still has some shortage, including the complex certificate management mechanism and the expensive certificate chain authentication mechanism. At the same time, due to the limited memory of mobile terminal devices, the mobile terminals do not store their own public certificate but the certificate URL, which brings security risk and revocation mechanism to the certificate [3]. And the recent scandal prism further reminds us that the information security products must be domestic.

So this paper proposes a mobile payment protocol based on the secure UIM chip. This protocol gives a full consideration to the mobile terminal's own characteristics: relatively low computing power, limited storage capacity, low processing capability and throughput sensitive to protocol overhead and compression [4]. And this protocol uses the domestic security chip, build the self-development security protocol based the existing UIM card, which applied the mobile payment process, so the UIM card based secure mobile payment protocol is established.

2. Analysis of Mobile Payment Protocol

Mobile payment is a kind of service method which allows users to use the mobile terminal to account payment for the consumption of goods. It is a new service channel after the bank counter, the self-service banking and online banking. Mobile payment includes proximity payment and remote payment. Proximity payment can achieve shopping, sign, bus cards and tickets and other functions by the mobile phone with NFC function. Remote payment is paid directly through paypal, online banking and other APP payment methods [5]. It is similar to the payment process on the PC side which completes the payment process through entering the account and password.

Mobile payment system typically includes four parts: the consumer (with mobile terminal), merchants, financial institutions and mobile operators. The specific procedures are as follows:

- The consumers use the mobile terminal to select the products and send the purchase order to the merchant.
- The merchant submits the consumer's purchase orders to the wireless carrier payment platform.
- The wireless carrier payment platform confirms the purchase order. The confirm instruction will be sent to the mobile terminal to request confirmation. If there is no confirmed information, the deal will be refused and the purchase process is terminated.
- Consumers send purchase confirmation order to the merchants.
- The merchants send the purchase confirmation order to wireless carrier payment platform and request the payment operation.
- Wireless carrier payment platform notify the financial institutions to make payments and settlement, and inform the merchants to provide services or goods. All the transaction records should be kept.
- The merchants provide goods or services, and keep the transaction records.
- Transaction ends.

In the above mobile payment procedure, the consumer's rights information, account information, transaction information and other sensitive data are required for secure transmission in the wireless network. And wireless carrier payment platforms or financial institutions are required to confirm the authenticity of the consumer's identity. At the end of the transaction, the consumers and the merchants cannot deny their own trading behavior. Therefore, the mobile payment process must meet the authenticity, confidentiality, data integrity, non repudiation and other security requirements, to ensure security of the entire mobile transactions smoothly.

3. The Research of Mobile Secure Payment Protocol

Through the analysis of existing mobile payment process, and the mobile terminal device and wireless network environment own characteristics, this paper proposes to build a secure mobile payment protocol based UIM card. The lightweight authentication technology and lightweight digital signature technology are used in the secure protocol to confirm the mobile terminal's identity in the mobile payment process, and to protect the sensitive transaction information.

The secure architecture of mobile payment protocol includes the two parts. One is the mobile terminal with

secure UIM chip, and the other is authentication center.

This mobile payment secure protocol uses the UIM secure chip at the mobile terminal. The key seeds should be preset in the secure UIM chip by the mobile carriers unified, and the key seeds are corresponds to the mobile user uniquely. The authentication, signature and encrypt operation are running in the secure UIM chip. The authentication center is deployed in the wireless carrier payment platform. The center is composed of the authentication server and the encryption card hardware. The authentication center is responsible for the authenticity of the mobile user's identity, and signs and encrypts the transformation data to ensure the data's confidentiality and non repudiation.

In the authentication process of consumer's identity, the mobile terminal get the time stamp at first, then the APDU authentication command is sent to the secure UIM chip. The secure UIM chip calls the light-weight authentication protocol according to the command. The authentication protocol calls the CSK (Combined Symmetric Key) algorithms [6] to generate the authentication password according to the secure parameters including the time stamp and the random number. The random number used is generated by the hardware random number generator by the chip itself. This authentication password is valid only in this transaction, and is invalid immediately when the transaction ends. The authentication password is sent to the wireless operator payment via the mobile terminal, and forwarded to the authentication center. The authentication center determines whether the consumer's identity is true or not, and returns the authentication results to the wireless operator payment platform.

In the sensitive transaction data transmission process, the mobile terminal will encrypt the data. The time stamp parameters and APDU signature and encryption instructions are sent to the secure UIM chip. Secure UIM chip receives the instruction. It will call the light weight signature encryption protocol to encrypt and sign the data, and the results encrypted and signed are returned to the mobile terminal. The mobile terminal will transmit these data to the wireless operators payment platform, further they will be transmitted to the back-end authentication center. The authentication center call the server-side signature verification and decryption protocol to verify and decrypt the data transmitted. Finally the results will be returned to the wireless operator payment platform, and it will perform the subsequent mobile payment process.

Mobile security payment protocol based on the secure UIM chip is as follows:

- The authentication center is in the back end of wireless operator payment. All the key seeds information for secure UIM chip of mobile terminals are encrypted and stored in the center. The store key used to encrypt the key seeds is stored in the encrypt card hardware. The wireless operator sends the key seeds in the form of secure UIM card to the mobile terminal user.
- Consumers use the mobile terminals to select goods, and send the purchase order to the merchant. At the same time, the mobile payment component of mobile terminal calls the lightweight authentication protocol of secure chip to generate the authentication password. The authentication password and purchase order are sent to the merchant.
- Merchants will submit the consumer's purchase order and the authentication password to the wireless operator's payment platforms.
- Wireless operator payment platform will transmit the authentication password to the authentication center at first. If the authentication process succeed, the payment platform will send the purchase information commands to the mobile terminals to request confirmation; If the mobile terminal does not return the confirmed information, the payment platform will refuse the trade and the purchase process is terminated. If the authentication process fails, the purchase process is also terminated.
- Mobile consumers call the secure UIM chip to sign and encrypt the transaction information. The encrypted transaction and the purchase confirmation order are sent to the merchant.
- Merchants will transform the encrypted transaction information and confirm information to the wireless operator payment platform, request payment operation.
- Wireless operators payment platform receives the transaction signature information and cipher data, and transforms them to the authentication center. The authentication center decrypts the information and verifies the signature. If signature verifies succeed, the payment platform will notify the financial institution to account for the payment between the consumer and the merchants. Then the payment platform notifies the merchants to provide services or goods and the transaction records are kept. If the validation is not passed, the consumer's transaction information is mainly tampered. The purchase process stop.
- The merchants supply the goods or service, and keep the transaction records.
- The transaction ends.

4. Analysis of Performance

4.1. Technical Realization of Secure UIM Chip

The design of secure UIM chip is the key technology of this project. UIM chip is a kind of phone card which is used to access the China Telecom CDMA network. The information stored in UIM chip includes user identification and authentication information, as well as business information relevant to the CDMA system. The ordinary UIM chip is similar to the SIM card, only provide the basic phone service function. Secure UIM chip mainly has the secure function, which supports the domestic symmetric algorithm. All the key related information, authentication protocol, data signature protocol and encryption/decryption etc secure protocol are written in the UIM chip.

The design of secure UIM chip needs the cooperation of UIM card vendors and secure chip manufactures. This project team designs the basic secure protocol and algorithm library. The secure chip manufactures is responsible for the bottom development of chip. Finally the UIM card vendors design the ADU instructions for the mobile terminal. In this model of cooperation, the suitable development method must be found, which is convenient for debug in the development process.

It is needed to point that the secure UIM chip based mobile payment protocol applies limitedly. It only adapts to the telecommunications users. Compared with the other SDK mode, the secure UIM chip based mode is more convenient for users. The SDK based secure protocol is easy to realize, but needs the additional SD card interface. As for the application promotion, the secure UIM chip based mobile payment protocol is executed by the operators and is more easy to promote.

4.2. Implementation of Lightweight Security Protocol

The mobile terminal has the following characteristics. a) Compared with the PC, mobile terminal's processor capacity is limited. The complex electronic payment protocol cannot be executed in this kind of processors. B) The storage space of mobile terminal is limited. C) The network band with is limited. D) The relatively low calculation and processing capacity. All these features put forward special requirements for the secure protocol applied in the mobile terminal. Traditional public key secure mechanisms are not suitable for the mobile terminal application. This paper puts forward a light weight secure protocol base on the symmetric key algorithms and CSK technology. This protocol is composed of light weight authentication protocol, light weight digital signature and encryption protocol.

The key technology of light weight secure protocol is that it occupied small space, computes fast and has high security. In the light weight authentication protocol, only dozen of bytes is used to finish the authentication of mobile terminal. The light weight signature and encryption protocol only use one key mechanism and a symmetric key to realize the signature and encryption process, the complexity is reduced. Due to the lightweight secure protocol is totally based on symmetric key mechanism, the computation speed is improved. At the same time, because the secure UIM chip's nature, the security is improved too.

5. Conclusions

This paper prompts secure mobile payment protocol. The specific security mechanism includes light weight authentication protocol and light weight signature encryption protocol. With the development of smart mobile phone and the scale of mobile users, the mobile payment business has been developed rapidly. The secure issues of mobile payment also increasing attracted the attention of the government, operators, mobile terminal manufactures and mobile phone users.

This secure UIM chip based mobile payment protocol can ensure the security of pre-trade, in-trade and post-trade. Before the trade, the mobile terminal's identity must be authenticated; In the trade, the transaction information must be signed and encrypted; And after the trade, all the secret information must be verified and stored securely. The real and effective identity, safe and reliable transaction data, and the non-repudiation of transaction information, all these ensure the secure mobile payment.

Acknowledgements

The authors wish to thank the helpful comments and suggestions from my director and colleagues in Beijing

Key Laboratory of Network Cryptography Authentication. This research is financially supported by Beijing Municipal Organization talents project (2013D002022000001).

References

[1] Enfo Desk (2015) 2015 Second Quarter China Mobile Payment Transaction Size Exceeded the Scale of the Internet Payment Transaction for the First Time. http://mt.sohu.com/20151014/n423220903.shtml

[2] Luo, X. (2014) Basic Principle and Normal Regulation of PKI Technique Apply. Computer Knowledge and Technology.

[3] Wang ,Y.W., Zhao, Y.S. and Zhang, H. (2013) Research on the Countermeasures for the Security Issues of Mobile Terminals. Designing Techniques of Posts and Telecommunications.

[4] Du, L.P., Guo, J.W. and Li, Y. (2013) Research on Micro-Certificate Base Authentication Protocol. Computer Science and Electronics Engineering.

[5] Wang, H.X., Yang, D.L., Jiang, N. and Ma, H. (2013) An Online Mobile Payment Model with Simplified Terminal Authentication. *Journal of Computer Research and Development*.

[6] Feng, F.W., Li, Y., Du, L.P. and Zhao, G.F. (2013) Design of Digital Signature System Based on Combined Symmetric Key. Network Security Technology & Application.