Research and design of NFC mobile payment based on Android

Zhizhou He, Yijun Liu

Faculty of Computer, Guangdong University of Technology, Guangzhou 510006,China

676340908@qq.com

Keywords: Near Field Communication; Secure Element; NFC shield;Global Platform

Abstract: For mobile payments using Near Field Communication,this paper summarizes weaknesses in its implementation by the Android Operationg System and vulnerabilities in hardware layer.a new NFC payment model is proposed using NFC shield in paper.this model is secured by design and can be implemented using existing specifications,technologies and hardware,his model can meets requests in safety and convenience of NFC mobile payment as well as the identity authentication function during payments.

Introduction

With development of mobile Internet, in recent years NFC technology get more and more industry attention[1], it's application brought great convenience to the people's life, NFC can provide easy, safe and quick of wireless communication technology, the technology is also applied in mobile payment, but it's security problem has attracted people's attention. Google, using an embed SE to stored cardholder data when desigin the scheme. SE has a high degree of security and tamper resistant implementation environment, in essence, SE is a CPU, can run the smart card application. A smart card also has a key algorithm for the co-processor, which can provides a secure execution module for the NFC technology.

NFC work in a very short distance, usually less than 10 cm, this design is considered to prevent the NFC wireless remote interface gice away card information, however, a relay attack will enable NFC interface caused by leakage[2]. In addition, SE access control is guaranteed by strict implementation of GP Se, however, this specification has weaknesses[4-5], will be subject to denial of service attacks (DOS) and produce unacceptable risk. Therefore, in order to solve the existing problem above, so that SE can not only ensure the integrity, payment security and usability and security payment process. In this paper, a new NFC payment model is proposed that is based on Android platform and NFC shield module.

Basic theory and shortage

NFC which full name is Field Communication Near ,it is short distance communication technology, the technology allows electronic devices contact point to point data transmission, its operating frequency is 13.56MHZ, 10cm, the main parameters and characteristics of the technology are shown in Table 1.

Tab.1. NFC main parameters and characteristics

frequecy	13.56MHZ
distance	0-10cm
speed	106,212,424,848 Kbit/s
patten	half-duplex
Copatibility	ISO14443A/B,Felica, IOS18092,ECMA340,352, 356,ETS
mode	passive，active

NFC has advantages: firstly, NFC can provides an easy, safe and speedy communication by wireless connection technology[3], it's transmission range is smaller than the RFID, RFID can

© 2016. The authors - Published by Atlantis Press

reach several meters, or even tens of meters, but NFC take the signal attenuation, respect to RFID, NFC is short distance, high bandwidth, low energy consumption; secondly, NFC can compatible with existing contactless smart card technology[6]. Now it has more and more manufacturers which support the formal standards, compared with other wireless connection, NFC is a short distance private communication.

However, this short distance payment also has hidden dangers, although the scope of work is short, respect to other wireless technology ,NFC is more secure but also will be threatened by a relay attack, which involves the security of authentication, the model proposed in this paper is a reliable verification scheme, can improve the security of the transaction more effectively.

The new NFC mobile phone payment scheme

There has a hidden trouble: stolen brush. In England ,a fraudulent events has happened and Malicious person make mobile equipment transformed into a POS machine, and sweep NFC enabled mobile devices nearby, in case your storage in se will be Pirates of the brush. This is a very serious accident. Causing such an event , because the NFC payment process did not do a good job in the identity verification measures. This paper proposes a new method of authentication in NFC payment, using a device similar to the U type shield, which is referred as "NFC shield" ". now introduce the structure of the module.

The NFC shield that proposes in paper is same as U type shield, it consists of the CPU and logic encryption, ram, ROM, EEPROM, I/O, Otg interface, led and two button. The operation use of the smart card chip operating system (COS), the component such as shown in Figure 1, and be same as U type shield ,it is based on PKI technology, and use 1024 bit asymmetric key algorithm of data encryption, decryption and digital signature.

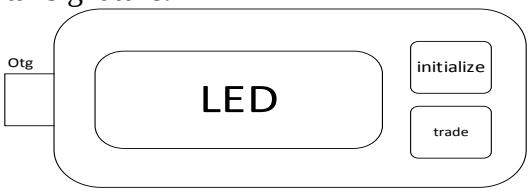

Fig.1.NFC-Shield architecture

From the picture, NFC shield work model is divided into two types: the initialization mode and the transaction mode. a brief introduction of the two modes.

Initialization mode: the mode would generate a pair of public and private key, as shown in Figure 2, the specific steps are as follows:

(1) Mobile device can connect to NFC shield by the interface of the Otg.Press the button ,if it is first initialized, firstly,NFC shield judge mobile device has been installed driver or not, if you have installed, skip to step 2. Otherwise, the device will automatically receive the NFC shield application (the application for managing user pin code)[1], and installed in the mobile device.

(2) After installation of the application ,the mobile device will pop up a password window for input PIN code, if it is the first time to initialize, you must enter the same password two times, otherwise you just enter a correct PIN code.

(3) the NFC shield will generate a pair of public and private keys which is based on the PIN code and the unique identification code of the mobile device.

(4) after generate the key pair, the NFC shield will return the public key to the mobile device, and the LED screen will show "initial success", otherwise it will show " initial failure".

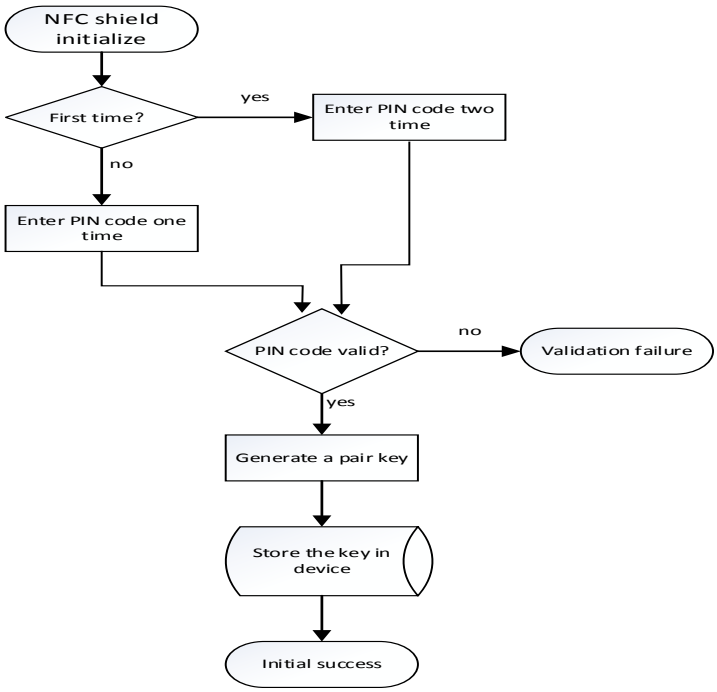

Fig.2.NFC-Sheild initialize procedure

Trading mode: the mode is work in NFC payment, In order enter the mode, the terminal and NFC shield must be connected through the Otg interface, in the transaction, the NFC shield will get the public key that is sended by mobile device to verify, the specific steps are as follows:

(1) After mobile device successful connect with the NFC shield by Otg interface, the mobile device sends a public key to the NFC shield.

(2) Receiving public key, the NFC shield carry out the asymmetric decryption algorithm to decryt the key, the process is performed only in the chip, so the security of the authentication is ensured.

(3) After decryption operation is completed, the NFC shield will return message to mobile device , if the result is 6600, it is success,NFC will unlock so that it can go transaction,and the LED screen will display "Pass verification ,can carry out transaction" , otherwise ,it could not complete the transaction, the LED screen display" Validation does not pass, can not carry out transactions ".

By explain above , the NFC payment security will be greatly improved[6], the NFC shield module can prevent stolen brush risks effectively, as shown in Figure 3 (b),if mobile devices have not link up with NFC shield, it can not unlock NFC lock.

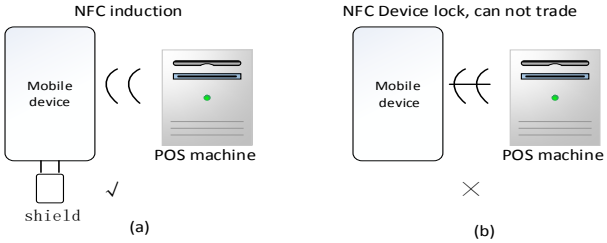

Fig.3. NFC-Sheild trading process

Conclusion

The design never increase operation difficulty, compare to wechart and Alipay mobile payment, see Table 2, the paper design will be more easy, the transaction process also take current NFC mobile payment advantages,it does not need to input the password while transcation, by instead, insert NFC shield as the authentication, payment security can be obtained further protection.

Tab.2. Comparison of three kinds of payment methods

	Current NFC model	Wechart/Alipay model	NFC shield model
operability	easy	easy	easy
security	high	high	More higer
Payment efficiency	quick(about 1s)	nomal(need to be online 15s)	quick(about 3s)

Acknowledgment

It is a project supported by the National Natural Science Foundation of China (NO:6116019).

References

[1] Chen Xi.Terminal Security of Mobile Finance.Thoughts Contending:106-110(2014)

[2] Waqar Anwar, Pavol Zavarsky, Dale Lindskog, Ron Ruhl.Redesigning Secure Element Access Control for NFC Enabled Android Smartphones using Mobile Trusted Computing.Information Society(i-Society), 6(24-26):27-34(2013)

[3] Pascal Urien.A secure cloud of electronic keys for NFC locks securely controlled by NFC smartphones.Consumer Communications and Networking Conference, 1(10-13):1120-1121(2014)

[4] Yang Chen,Yang Jian-jun.Research on the Technical System and Standardization of Security Assurance for Mobile Payment. Information Technology & Standardization, 7(1):17-20(2010)

[5] Wu Yi-ming,He Jia-rong.The Design and Implementation of the SQlite Security Mechanism Based on Android and Remote Service.Journal of Guangdong University of Technology, 30(3):49-52(2013)

[6] Luo Ming-yu,Ling jie.A Security Cloud Storage Scheme Based on Cipertext Policy Attribute-based Encryption. Journal of Guangdong University of Technology, 31(4):36-40(2014)