Research and analysis of NFC mobile payment security

Zhizhou He[a], Yijun Liu

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

[a]676340908@qq.com

Keywords: NFC mobile phone payment; potential safety hazard; security

Abstract: This paper analyze the development of NFC mobile phone payment, and elaborates the concept of NFC, discuss some technical problems in latest.Be directed against every layers of technical security problems in this field.

Introduction

In recents,There are various mobile payment methods has emergence: telephone banking, Alipay, wechat mobile payment, when every kind of payment launch, they called the mean of payment is safe, however, for users, payment security is the most important factor to make a selection[1-2], therefore , each payment should pay more attention.

NFC is a new technology that has rapid development in recent year, this technology is a short distance communication technology between electronic equipment[3],and it also used in mobile payment, in public, security evaluation of NFC is good, but this does not mean that the technology has no security risks, especially the technique has become popular,so it need to pay attention to security issues.As security improves, promotion will be easier and faster.

This paper analyzes the security risks and it's security on the Android platform.

Basic theory

NFC device has three working modes:

Active mode: NFC terminal send its own radio frequency to identify and read/write other devices.

Passive mode: The NFC terminal is simulated as a smart card which can be read or write, it only take passive response in other equipment RF.

Bidirectional mode: each side take the initiative to send a radio frequency field to establish the point to point communication.

NFC mobile payment is to make the mobile phone in a passive mode, simulation into a smart card, and then carry out card payments. NFC payments need to have such Component: secure element is responsible for ensuring the payment system security, se can be fixed on the mobile phone or embed in the SIM card, SD card[4]; NFC front-end chip is responsible for wireless communication by connecting the antenna; OTA responsible for download and management payment application which storage in se.

SE played a vital role in payment . SE is a CPU card, that can run the smart card application. A smart card also has a key algorithm co-processor, which can support decryption algorithms (DES, AES, RSA, etc.). The smart card has many kinds of technology to realize the anti - attack characteristic, it is difficult to extract data from the chip.

SE can be variety of shapes,as shown in Figure 1, the paper only describes the four most cited:

Baseband processor: It is one of the most important part of phone, it control the mobile phone connection and manage applications to run, in order to provide high security , SE can be as a baseband memory module, so the phone does not require to modify, and this form can avoid the user to add an additional hardware to use SE to provide security services, however, mobile phones once lost, damaged or exchange, SE module should be transformed, so far this model did not become mainstream.

Embed SE : SE module welded on the phone, so it can't be removed. However, this chip is embedded on the phone in production phase, when the device is delivered to the user, must be personalized, which means will indirectly increase the price of mobile phones. This form of SE, can not be used by other mobile phones, when the transformation of the phone, you must redesign the chip, and now, this model has not become the mainstream.

SD card form: it composed of a memory card and a smart card. Therefore, this form of providing the same security of smart cards and can meet majority,it can be removed, and has a large storage space, when the user change phone, it does not need redesign, but not all mobile phones have SD slot, therefore, this form has not become the mainstream[5].

UICC form: This form is removable, that SE module is embedded into the SIM card, because it is attached to the SIM card, the security has been further improved, and also own security mechanism of SIM card, and now, China Mobile and China Unicom are used in this form.

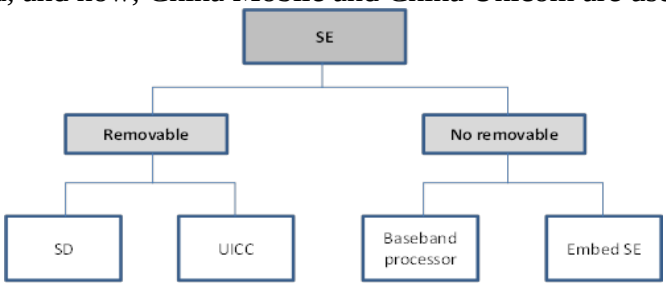

Fig.1. Various SE forms

Conclusion

Table 1 summarizes evaluation criteria above, we can conclude that baseband processor form is the most unacceptable, it is certainly due to his practicality; for the embed SE, the weakness is poor reusability, however, this form is also can be transition types, some banks, they are willing to use an independent way, without sharing security domain; SD card form is generated independently from the bank and the mobile terminal that they can not reach a fair NFC ecological system, and it can be reused, but not all mobile phone have SD card slot, such as iphone; UICC form can be the best choice for NFC ecosystem today, in addition to its reusability, its safety have been verification, normalized, In the promotion of the stakeholders, this form has been the most widely used

Tab.1.The criteria of NFC

Criterion / SE Form	Security	Reusability	standard	sums
Baseband	+	–	–	–
Embed SE	++	–	+	++
SD form	+	++	+	++++
UICC form	++	+	++	+++++

Safety analysis

The security of the NFC mobile payment, major industries are in effort, they are trying to cooperate so that it can improve security.

This papaer analyze the whole process on the payment of current NFC mobile analysis it’s security, hoping to provide a reference for future development of this field.

As shown in Figure 2, showing the details of the various channels from the software layer to the hardware layer, the NFC mobile payment, based on it, this section will be involved in the security to analysis.

This paper mainly analyzes SWP-UICC form of NFC, this form is mainly composed of NFC controller, SWP-SIM card, SE, application processor, baseband chip and RF antenna.

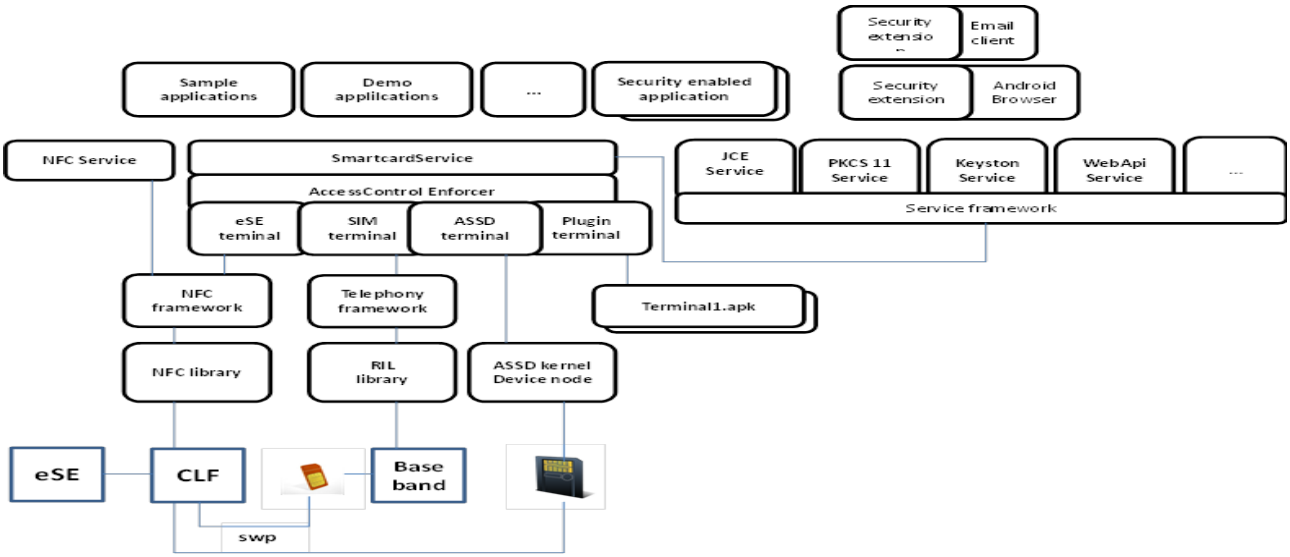

Fig.2. NFC payment protocol channel architecture

Security architecture of software layer

As shown in Figure 2,there exists a access control module (accesscontrol enforcer), namely, security access control module, the module using global platform credit framework of GPAC, that is compose by access control module with the UICC card rule file, and it realize to control and manage access privileges to the UICC card control, in order to avoid improper use of SIM/SE access interface that will harm to user.

If mobile app want to access UICC card, the access control module should match access rule ,and then based on the results of the matching to determine whether allow APP access, this process is as follows:

Firstly, we get the rule file from the security domain of UICC Card, and store the rule information in the mobile terminal.

Secondly, App using SIM/SE interface to open the channel that can interactive with the application which store in UICC card.

Thirdly, the access interface forwards the APDU request to the access control module by the APP.

Forthly, the access control module obtain the signature certificate for request terminal application.

Fifthly, Access control module to get TAG Refresh from the rule database; UICC return the updated tag, and compared them, it will take the two measures according to the results.

Sixth, Return the result to the transport layer module. If result is not allowed, return the error to the terminal. If the license is permitted, the response will be returned.

Seventh, If the app is allowed to access, the UICC access interface will sends the APDU to the UICC.

Security architecture of hardware layer

In hardware layer, NFC mobile payment add a SE module, the module play an importance role in payment, the important private information will stored module.

SE is a CPU, it can run smart card applications. It contains ROM, EEPROM, RAM, CPU and I/O interface,SE has AES CO-PROCESSOR, TRIBLE-DES-CO-PROCESSOR and PUBLIC KEY CO-PROCESSOR enhanced that can support AES, DES, RSA encryption and decryption algorithm[2], SE module mainly to prevent external malicious attacks to protect data security.

SE module is connected with devices by S2C interface. S2C interface is security encryption interface of NFC wireless communication by two line connection: Sigin input line and the Sigout output line, Sigin can provides SE chip data for the NFC module, Sigout can provide the clock and data for SE chip. In above, NFC chip connect NFC device by the wireless sensor and then connect

SE chip by S2C,the design is intent to avoid the malicious intercept private data when in transmission.

Conclusion

In the software layer and hardware layer, NFC technology use the advanced technology to ensure the security.In hardware layer ,it defined as a short distance communication, and has Several security modules in the hardware architecture, which makes the NFC technology is guaranteed in hardware, the software layer take some agreement to ensure its security, combination of software and hardware, it make hard to crack this technology , Though the security is good, it does not mean that it can not cracked, especially it relate to electronic transactions,so it need to do research continually.

Acknowledgment

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

References

[1] Marechal.Juin,Secure Payment with NFC Mobile Phone in theSmartTouch Project,IEEE.12(2008)

[2] Dhaka.Bangladesh,Secure Mobile Communication,In m-Payment system using NFC Technology[C],IEEE(2012)

[3] Surya.Michrandi.Nasution, Prototype of Train Ticketing Application Using NFC Technology On Android Device[C],International Conference on System Engineering and Technology, 11-12(2012)

[4] Szu-Hui.Wu, Promoting collaborative mobile payment by using NFC-Micro SD technology,IEEE,10th International Conference on Services Computing(2013)

[5] Hasoo Eum, Conditional Privacy Preserving Security Protocol for NFC Applications,IEEE, (2013)