Fraud on host card emulation architecture: Is it possible to fraud a payment transaction realized by a mobile phone using an "Host Card Emulation" system of security ?

Marc Pasquet, Sylvie Gerbaix

Fraud on Host Card Emulation architecture

Is it possible to fraud a payment transaction realized by a mobile phone using an "Host Card Emulation" system of security ?

Marc PASQUET
Full professor at ENSICAEN
Member of GREYC laboratory
Caen, France
marc.pasquet@ensicaen.fr

Sylvie Gerbaix
Associate Professor at Aix Marseille University
Member of Montpellier Research in Management lab.
Montpellier France
macsy2@wanadoo.fr

***Abstract*—Mobile payment transactions with a NFC device are secured by two main architectures. The first is in using a "Secure Element" included in the mobile phone, the second using an external "Host Card Emulation" architecture where the banking card emulation is realized in a grid connected by the air to the mobile phone. That last solution seems to be the preferred solution today. Is it possible to fraud this type of transaction?**

Keywords-component; Fraud, NFC, HCE, Host Card Emulation, Mobile payment, security

I. INTRODUCTION

Mobile payment transactions with a NFC device are secured by two main architectures. The first is in using a "Secure Element" included in the mobile phone or using an "Host Card Emulation" architecture where the banking card emulation is realized in a grid connected by the air to the mobile phone. That last solution seems to be the preferred solution today. We will try in this paper to show that exists at minimum one solution to overpass the securities. So in the first part we will present the NFC / HCE solution of payment, and in a second part the possible attack on the system.

II. PAYMENT TRANSACTION WITH HCE

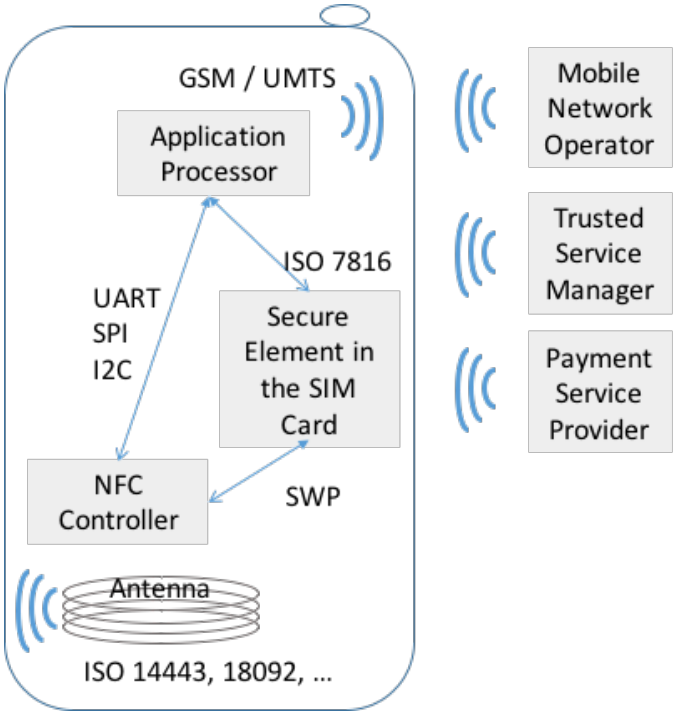
A. The NFC payment protected by a Secure Element

The massive emission of cards without contact has contributed to the notoriety of the payment without contact NFC realized by a mobile phone. The payment NFC is currently bases on a Secure Element (SE): mainly included in the SIM card, which belongs to the mobile operator. This solution is a great source of constraints for the payment service provider. To cure it, the actors of electronic moneys created the HCE (Host Card Emulation).

For understanding how does the HCE operated, it is important to point out that of the current model: the SE is embarked in the mobile.

Mobile payment NFC "classical" is a payment where the smartphone serves as credit card. Antenna NFC allows the smartphone to dialogue with the electronic payment terminal (POS). Controller NFC will request the SE (often the SIM card, and this solution is called "SIM-centric") who contains the significant banking data card number called also PAN (Personal Account Number, Validity Date, cryptographic keys, …). At any moment, the mobile Phone Operating System is not aware of these data. It is there that the robustness of NFC SE, resides.

The SE in the SIM card complicates, the installation of the payment application as well for the Mobile Network Operator as for the Trusted Service Manager as for the Payment Service Provider,.

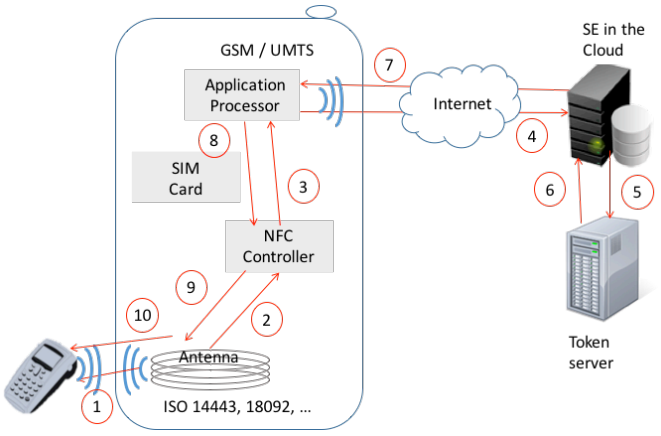


Conceptually, the technology of the HCE allows the de-synchronization of the NFC with the SE lodged by the mobile; the operating system (OS) pilot thus directly the NFC. In its most primitive form, the mobile phone application installed in OS can protect the banking data in the Secure Element.

B. *The banking data in the cloud*

But technology allows things much more interesting like storage the banking data in the cloud, like in the "HCE" solution.

In addition, in order to limit the risk of recovery of the significant data by a malware carried out in the memory of the mobile phone, the engineers had the idea to generate disposable card numbers. This security is called "tokenisation". The latter was the object of a specification by the EMV Co organization making it possible to ensure interworking. Initially, we will explain how the HCE functions when the smartphone is connected to the network, and when it can go to seek the data in the cloud.



When it approaches of the POS, the smartphone will solicit, via the antenna NFC ①, the controller NFC ②. This one uses his table of management of the application Identifier (AID) in order to know where to send the request without contact. If the AID is present in the table, the request will be sent directly to the SE (case of the model "SIM-centric"). If not, it will be transmitted to the application lodged in the operating system of the telephone ③. Then the application manages the possible call of the SE in the cloud (HCE) ④ in order to send the data sensitive to the controller who will transmit them in NFC to the POS ⑦⑧⑨⑩. For more security, certain data, (Personal Account Number, Validity Date, cryptographic keys, …), can result from a token server ⑤. This last generates disposable numbers thus preventing any re-use of the same data ⑥.

C. *Disconected mode*

Previous kinematics presupposes that the telephone is connected to the network, if not the cloud will not be accessible. In order to always allow the use of the payment via HCE, the management of the disconnected mode made its appearance. For that, the application communicates, upstream, with the token server in order to download card numbers which could be used when the network is inaccessible.

D. *Installation*

Contrary to the mobile payment presented SIM centric, the subscription of a card holder for an application being based on technology HCE is easy. Indeed, with the HCE, there does not need necessarily TSM to install an application in the SE. A simple classical download since the store will be enough.

III. WHAT ABOUT SECURITY?

A. *Attack on the telephone data*

The fact that the significant data go back to the operating system is dangerous from a security point of view. In order to limit the risk, the HCE server protects the transmission from the data towards the mobile phone by a secure channel (symmetrical cryptography between the mobile phone and the server). Moreover, the server HCE carries out a recognition of the mobile phone (IP address and Mac address) and sends the data only if this recognition is positive.

It would thus be necessary to protect these three elements, symmetrical key, Mac address and IP address. Indeed, the appearance of a malware within the smartphone, would allow recovery of the aforesaid data even if those data are well protected [4] [5].

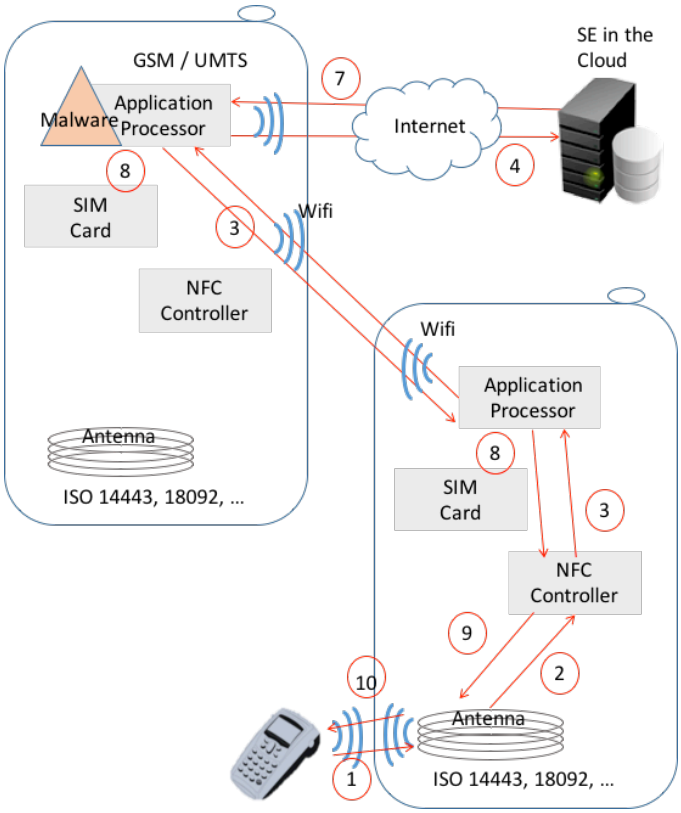
If these security data are compromised, it will be possible to use an other mobile phone in place of the right one, to obtain the significant data of the payment transaction.

B. *Attack between the application processor and the NFC controller on the mobile phone*

But another attack is possible. If the malware transfers the significant data of the payment transaction, once this one obtained, towards another telephone. This last will then have the possibility of carrying out the transaction with the data obtained, without neither the genuine holder was informed of this attack nor the HCE server.

This attack is much more possible if the application uses the disconnected mode but not only.

The problem is mainly related to the mobile phone OS, which is not sufficiently made safe in the event of loading of Malware on the telephone. Specialized servers in this kind of attack already exist in the USA [6].



To limit the risk, mechanisms of security take part thus in the security of the HCE, as the tokenisation which one already approached. But there are other mechanisms as the scoring in order to know if an authorization EMV must be emitted by the issuer or not.

IV. CONCLUSION

We have presented in this paper two solutions of attack and two solutions to protect the HCE architecture.

Moreover we have to see whether technology HCE will be sufficiently robust for a long time. Will the wild imagination of the hackers manage to fissure this technology? As many questions which will remake surface as the emergence of the emulation of lodged cards.

ACKNOWLEDGMENT

Thank you to “Carte Bancaire” organization (France) for their precious advices.

REFERENCES

[1] MasterCard PayPass – ISO 14443 Implementation Specification Version 1.1 – March 31, 2006

[2] Esko Strömmer, Mika Hillukkala, Arto Ylisaukkooja, “Ultralow Power Sensors with Near Field Communication for Mobile Applications”, IFIP (International Federation for Information Processing) Volume 248, 2007, pp 131-142.

[3] EMV 2000 specifications can be found at http://www.emvco.com/specifications.cfm

[4] R. Anderson, “Why Cryptosystems Fail,” Comm. ACM, Nov. 1994, pp. 32-41.

[5] A. Pfitzmann et al., “Trusting Mobile User Devices and Security Modules,” Computer, Feb. 1997, pp. 61-68.

[6] Dominik Haneberg, Wolfgang Reif, and Kurt Stenzel, “A Construction Kit for Modeling the Security of M-commerce Applications”, Lecture notes in computer science, Volume 3236, 2004, pp 72-85.