The Complexity of Security Studies in (NFC) payment System

Marc Pasquet, Sylvie Gerbaix

The Complexity of Security Studies in NFC Payment System

Pr. Marc Pasquet[1] and As. Pr Sylvie Gerbaix[2]
[1]GREYC CNRS UMR 6072 laboratory
Higher Education National Engineering School of Caen, France
[2]CREGOR Montpellier University II, France
[1]marc.pasquet@ensicaen.fr
[2]macsy2@wanadoo.fr

Abstract

If we compare the security problem of a face-to-face contactless card payment process with a mobile phone NFC payment process, we may easily consider that the latter is far more difficult to study. Indeed, the more partners from different organizations involved in the process there are, the more complex the studies are and, accordingly, its protection. As well as the current solutions applied to studying the electronic payment security chain (Common Criteria, ISO 27005, etc), the James Reason model has pointed out the specific risks implied by the interaction between the different links in a complex chain. His theory has been applied to various fields (airplanes, nuclear power plants, health, etc) and various ways of studying it have been proposed. In this article we will attempt to apply his model to the complex electronic payment chain required by the NFC payment process.

Keywords

Electronic payment, Contactless card, NFC, Security chain analysis, the Reason model

INTRODUCTION

The purpose of this article is to contribute to the study of security aspects of electronic payment using a new approach. We will focus on electronic payment architecture because, today, this architecture involves more and more partners and we can consider that the financial stakes complicate the analysis of the traditional axes in information security: Confidentiality, Integrity and Availability.

The regular smart card payment process respects the EMV (Europay, Mastercard, Visa) specifications and can be considered today as reasonably secure (Pasquet, 2008). The percentage of fraud in face-to-face payment with an EMV smart card, is around 0.05%. But new types of payment are being more and more commonly used.

Originally, contactless payments with chip cards were introduced. This process is very close to the EMV smart card payment process, except that, instead of wires, there is a radio link between the card and the POS (Point of Sale). However, as the distance allowed is very short, the possibility of fraud is higher than with EMV payment, although only slightly higher as there are no new partners involved in this process. In spite of this, banks reserve that particular type of payment to small amounts (less than 20 €) for security reasons. The PIN code is not typed by the cardholder, on one hand because the radio link is less secure than a wired connection and, on the other hand, because it is more complicated and payment takes more time (the cardholder must present the card, type the PIN code on the POS keyboard, and present his card again, etc).

Later on, NFC payment appeared. NFC payment looks like a contactless payment but a new type of mobile phone handset replaces the contactless card. The banks are less sure about security than with a contactless card due to involvement of new partners. The process involves two supplementary main partners: the handset manufacturer and the mobile phone operator. Both of these are as important as a card scheme, and their security policies are driven by the phone market and not by the payment market. Both of them respect the general card scheme specifications, but they are more difficult to manage than the POS manufacturers (who are completely tied to the payment market). Banks therefore limit this kind of payment possibility. In this article, as an example, we will take an applied method used by certain banks in the world. If the SIM card (UICC) is able to make small payments (20 € max) via the mobile phone handset, then after four or five times (or Σ = 100 €) the payment application triggers off an authorization request, to the issuing bank to check whether that SIM card has been stolen. In fact, the “base band”, of the mobile phone, includes a POS emulator and, via GSM, calls an OTA platform (belonging to the telecom operator), which is connected to the authorization bank's server.

Although contactless payments are being used more and more in several markets (US, UK, SEPA in Europe, etc), NFC payments are still in the prototype phase and, for security reasons, are not generalized apart from in Japan, where the telecom operator, handset manufacturers and banks, work together easily.

In fact, we can consider that these innovations in electronic payment processes tend to increase the number of elements involved and their diversities: organizational partners, users, and devices, and the current security analyses are focused on the security of each element in the whole electronic payment chain. Consequently, end-to-end security analysis is difficult for two main reasons: the security policy of each partner may be different, and the interaction between the different devices may create a gaping security hole. James Reason has identified and pointed out that these interactions imply specific risks, and has proposed ways of studying them.

In the first part of this article we will describe the security aspects of NFC payment. Next, we will focus on the current methods for studying end-to-end security for this type of problem. After a short presentation of the James Reason model, we will try to show how a new approach using Reason's model (Reason, 2000) can help us to cope with the complexity of the NFC security problem. Finally, we will conclude our research presentation.

THE COMPLEXITY OF THE CARD PAYMENT MODEL AND ITS SECURITY CHAIN

In order to point out specific security risks, we can consider that the reference, in the payment chain, is the "traditional" face-to-face model of payment by card. As we pointed out in the introduction, this type of payment is considered by banks today as almost secure. According to the Card scheme specifications (MasterCard PayPass Europe or Visa PayWave Europe), the banks are implementing these new payment solutions all over Europe. However, banks are less confident about EMV payment security and therefore limit the possibilities with contactless cards (no withdrawals and only small amount payments).

In this system of payment with contactless cards, as described in Figure 1, the main partners are:

- On one hand, the cardholder and his smart card, the card manufacturer, the issuing bank and the Card scheme, who certify and co-brand the card.
- On the other hand, the merchant, the POS manufacturer, the acquiring bank and the Card scheme who certify the POS and payment chain.

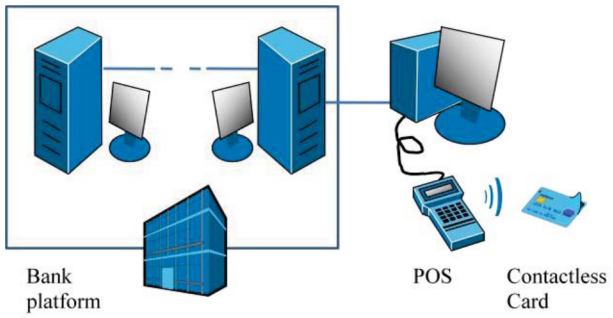

Figure 1: Contactless payment architecture

Banks consider bank platform security (including interbank links) as correctly secured and as having the same security policies. The merchant POS is certified by the card scheme, as well the issuing card. Personalization companies (EMV standards) and POS manufacturers (PCI PED standards) respect card scheme security policies. The acquiring banks lead the merchants through the card scheme policy by using the PCI DSS standards (EMV, PCI DSS and PCI PED standards are issued by the Visa and MasterCard card schemes).

With more recent and innovative NFC card payment systems, as described in Figure 2, the problem is slightly different.

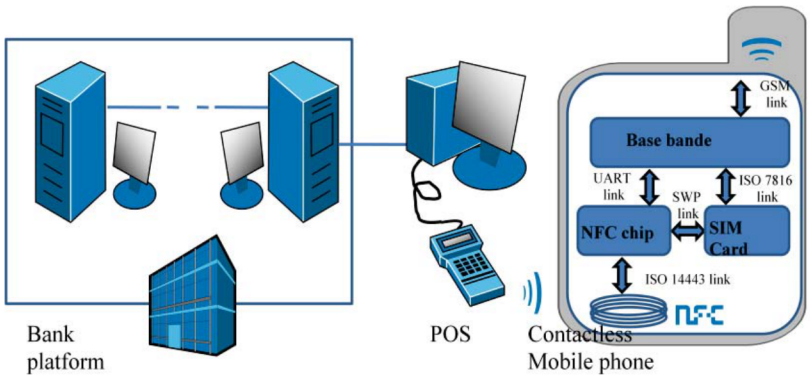

Figure 2: NFC payment architecture

To the traditional partners, with the mobile phone NFC payment process, a few others are added:

- The telecom provider who issues the UICC card (which can be considered as a smart card).
- The handset provider (mobile phone handset which can be considered either as a POS or a smart card).

The payment process can be described as follows:

- The SIM card (UICC), via the mobile phone handset, is able to make small amount payments (20 € max).
- After four or five times (or Σ = 100 €), the payment application triggers off an authorization request to the issuing bank as shown one Figure 3.
    - The base band has a POS emulation and calls the OTA platform via GSM.
    - The OTA platform connects to the authorization bank server.

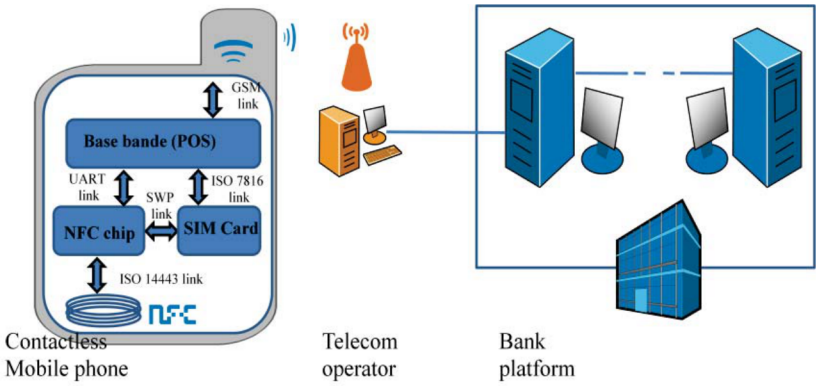

Figure 3: NFC authorization process

For contactless card payment there is only one safe type flow:

- For payment and authorization
  Chip -> Merchant POS -> Acquiring bank -> Card Scheme -> Issuing Bank

For NFC payment there are two safe types of flow:

- One for payment flow
  SIM -> NFC Chip -> Merchant POS -> Acquiring bank -> Card Scheme -> Issuing Bank
- One for authorization flow
  SIM -> Base band (POS emulation) -> OTA platform -> Issuing Bank

In terms of security, two domains are very difficult to certify (by banks or the card scheme):

- The NFC mobile phone which involves three main partners:
    - The handset manufacturer: mobile phone with base band, NFC Chip, keyboard, screen…
    - The SIM card (UICC): issued by a telecom provider and personalized, by a specialized company, with a Cardlet (include the software for banking payment)

    - The MIDlet manufacturer (MIDlet which emulates the POS, installed by OTA via the telecom provider)
- The OTA chain, which involves two main functions:
    - The MIDlet personalization
    - The Authorization flow

NFC payment with mobile phones involves far more partners than a face-to-face contactless card payment process. This increasing diversity of organizations involved in the card payment chain is supposed to be a factor of complexity and risk in the security chain. Consequently, in this article, the descriptions of security studies will focus on the security domain of each partner forming a layer. Each layer is characterized by its own culture in terms of security policy.

STANDARD MODELS FOR STUDYING THE SECURITY CARD PAYMENT CHAIN

In order to be more tangible in this analysis, let us take the example of a contactless card and a NFC phone. Both of these are able to make a contactless payment on an adapted POS, and they both follow the Java Card Global Platform specifications. However, there are certain differences:

- The **EMV** and PayPass or PayWave compliant payment application, is stored on the chip of the contactless card, protected by the **Global Platform** mechanisms, in a dedicated Security Domain (SD). A Common Criteria analysis is possible, because both cards and applications are issued from the same structure with one single security policy (**Common Criteria EAL 4 $^{+}$ or 5)**.
- The NFC-enabled handset supporting an UICC (SIM) can either offer GSM/UMTS services, send and receive calls, SMS, etc., or perform a payment acting as a contactless card. The payment application is stored on the UICC in the mobile phone; both of them use a dedicated Security Domain (SD). The independence between the payment application and the GSM application is managed by a software firewall provided by the Java Virtual Machine (JVM). This firewall prevents applications from exchanging information between one another. A common criteria analysis is very difficult to carry out because the IUCC card, payment application and handset are issued by different structures with different security policies.
    - The payment application embedded in the UICC must be certified as well as the chip (**Common Criteria EAL 4 +)** and must be **EMV** compliant
    - The developments must respect the **java Card global platform** requirements (Security Domain in Secure Element) and the UICC must be able to create a secure channel with the bank authorization server (Reveilhac, Pasquet, 2009). A Trusted Security Manager is necessary to separate the Telecom security layer and the bank security layer.
    - Base band POS applications must be certified by banking system (**PCI PED** and **PCI DSS** for the POS MIDlet, etc)
- The OTA must use the **ISO 27005** standard in a certification process that will be defined by card schemes or banks

Consequently, several major security policies are conducted. For example, in the latter model, the main layers (security domains) to be considered are:

- The banking field
    1. The Issuing Bank (Cardlet)
    2. The Client (account)
    3. The Card Scheme
    4. The Acquiring Bank
    5. The POS manufacturer
    6. The Merchant
- The telecom field
    7. The SIM (UICC) manufacturer
    8. The SIM Issuer
    9. The MIDlet developer
    10. The Mobile Phone manufacturer
    11. The OTA platform
- The trusted domains
    12. The Trusted Service Manager

These domains or layers belong to different partners each with specific policies. So far, the agreements (piloted by card schemes) between different banking domains, have led to a very high level of security. The new telecom security

domains, more oriented towards the telecommunication market and security (low price), and trusted security domains, with an awkward balance between banking and telecom requirements, are difficult to study, not only at the starting phase of the implementation, but, above all, throughout the whole duration of the NFC payment method.

REASONING WITH THE REASON MODEL

In a systemic approach to security studies, we may consider, according to the James Reason method (Reason, 2000, University of Manchester M13 9PL), that each partner has created certain defensive layers, and that these layers should normally be intact. “In reality, however, they are more like slices of Swiss cheese, having many holes, though unlike in the cheese, these holes are continually opening, shutting, and shifting their location. The presence of holes in any one "slice" does not normally cause a bad outcome. Usually, this can happen only when the holes in many layers momentarily line up to permit a trajectory of accident opportunity, bringing hazards into damaging possibility of security violation.” (Reason, 2000)

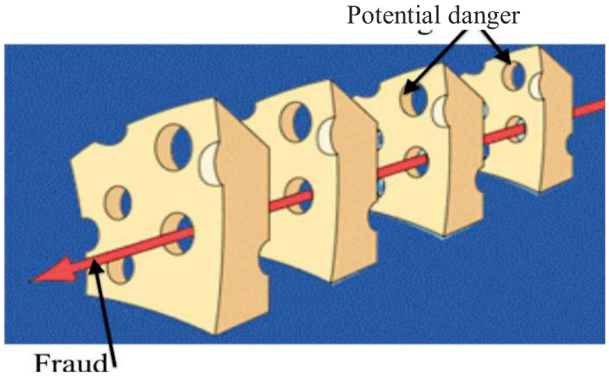

Figure 4: The Swiss cheese model (Reason, 2000)

The model distinguishes two different approaches to the problem of human fallibility: the person and the system approaches. “Defenses, barriers, and safeguards occupy a key position in the system approach. High technology systems have many defensive layers: some are engineered (alarms, physical barriers, automatic shutdown, etc), others rely on people, and yet others depend on procedures and administrative controls.” (Reason, 2000)

Following Reason’s model, a security analysis can be carried out in two ways:

- By identifying and remedying “latent conditions” **before** an adverse event occurs. Understanding this leads to proactive rather than reactive risk management and should be very important for the future of NFC, and help to construct the necessary tools (ISO 27005, PCI, etc)
- By investigating the causes **after** the occurrence of an adverse event, and modifying the devices or process accordingly.

The Reason model is progressively being used more and more to analyze risks and error management:

- In complex and risky Organizations (US Navy nuclear aircraft carriers, nuclear power plants, air traffic control centers, etc) (Scarborough, Bailey, Pounds, 2005) (Wiegmann, Shappell, 2003),
- After an Accident (aircraft accident, railways accident, etc) (Johnson, Botting, 1999),
- In the medical field (hospital, etc) (Lederman, Parkes, 2005)

Electronic payments are still not in the focus and it seems profitable to investigate in that direction. However, although the James Reason model would appear to be a useful model to assist fraud investigation analysis, it is only one component of the analytical process.

THE REASON MODEL AND NFC PAYMENTS

If we try to apply the Reason model to electronic payments, we may consider, in a macroscopic approach, that the different security domains are the different slices of the Swiss cheese.

The problem, pointed out by the Reason model, is that security holes are continually shifting their location. This means that, for contactless payment, an architecture constituted by banking security domains (or layers) conducted by card

schemes (Visa, MasterCard, CB…) which issue security rules and certification methods, is much more easily watched than the NFC architecture which involves banking and telecom security domains.

As we have shown previously, in the case of NFC payment systems, each layer is created and operated by a partner belonging to an organization which has developed its own security rules. These rules evolve according to different processes and the holes in the "slices of cheese" (security domains or layers) move separately with no conductor to harmonize the different partners. Sooner or later the holes will line up.

In our case, there are two major problems for banks: the first one is that in NFC payment the risk is mainly created by fraud, and the second one is that banks remain responsible for payment risks, and neither the telecom operator nor the handset provider are responsible for these payment risks. Moreover, modifying a mobile phone handset can take time. How much money will the banks have lost before those modifications are made?

According to Reason's model, then, in order to pay securely with an NFC mobile phone, several technical and organizational conditions will have to be respected before starting a general implementation:

- The mobile phone handset must be able to resist against physical attacks and logical attacks. Mobile phones (both hardware and software) must therefore be able to be certified by the card schemes.
    - In order to combat physical attacks, specific components can be used:
        - To reach level 4 (or higher) in common criteria, the ideal solution would be for all the functions of the mobile phone to be carried out with a single, well protected chip (System In Package).
        - To protect the PIN, one solution may be to use some kind of chip sealed under the PIN pad to encrypt the banking client PIN.
    - In order to combat logical attacks, two layers must be protected: the Operating System and specific payment software. A lot of good ideas are being developed today, and often mix hardware and software solutions:
        - A few Operating Systems, like Android, include a security process to fight the fraud.
        - The chip (System In package) has a cryptographic section to verify software signatures (action carried out before the start of each process).
        - A Secure Access Module (SAM, a sort of SIM used for cryptographic operations) is set in a two mobile phone SIM slots to in order to check the software signatures.
        - The SIM card (UICC) is Java Global Platform compliant and a secure element, in that chip (with Security Domains), makes the payment transaction secure.
        - Etc.

As regards human conditions, it will be necessary to initiate advertizing campaigns focused on the bank clients, concerning the best practices in NFC payment transactions and to train the partner's staff to fight against this specific type of fraud.

Beyond all these considerations, the Reason model is very interesting because, in the causal sequence of human failures leading to an accident or an error, it includes both "active failures" and "latent failures":

- The concept of active failures encompasses unsafe acts which may be directly linked to an incident, such as "client errors" i.e. giving one's PIN code to unknown person (phishing on the Web, camera on ATM, false phone call from the police …).
- The concept of latent failures is "particularly useful in the process of investigation, since it encourages the study of contributory factors in the system". For example with fraud investigations in NFC payment, an unsafe decision to make changes on the mobile phone in order to better match a new market (OS changes for example) which make it possible for a hacker to pick up the client's PIN code with a mobile phone spy virus.

Investigating the cause of fraud in NFC payment transactions should make it possible to identify active failures and latent failures within the defensive layers: technical, human, procedural and administrative. As a banking partner, modifying the devices, process or card scheme will require a permanent analysis of the point of fraud due to NFC payment methods, and a thorough investigation of the different cases of fraud. As a banking partner, modifying the devices, process or card scheme will require a permanent analysis of the point of fraud due to NFC payment methods, and investigate the different cases of fraud.

CONCLUSION

In order to reach a fraud rate for NFC payments close to that of contactless card payments, large modifications on the three main aspects in the system approach, pointed out by James Reason (Reason, 1997) as shown in Figure 5, are required.

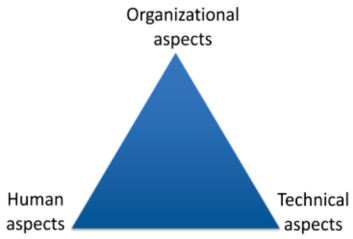

Figure 5: The system approach

Reason's model gives us many ideas for organizing high technology systems, both before and after the occurrence of a fraud event. His model is characteristic of highly complex organizations with many defensive layers, and very demanding in terms of security, as well as electronic payments in the core of the banking system.

James Reason has brought to light some paradoxes of high reliability. To cope with high risk situations (in electronic payment, fraud could be a cause of bank going bankrupt), organization managers have two contradictory demands: on one hand, timely human adjustments to react quickly to the new situations created by fraud attacks and, on the other hand, to establish specific procedures in order to avoid human risks of fraud. Because of these paradoxes NFC payment will have to find the right balance between these two poles.

Finally, the main problem of the evolution, from contactless card payments to NFC payments is that, in the former case, there is a homogeneous security culture (shared by all the banking systems) and in the latter case a heterogeneous security culture (the culture of the banking system and the culture of the telecom system). According to James Reason's argumentation, this heterogeneity might be a way of creating constant security violations.

REFERENCES

Johnson C.W. & Botting R.M., (1999), "Using Reason's model of organizational accidents in formalizing accident reports", *Cognition, Technology &Work*, 1:107-118, Springer-Verlag.

Ledermann R.M & Parkes C. (2005), "Systems Failure in Hospitals – Using Reason's Model to Predict Problems in a Prescribing Information System", *Journal of Medical Systems*, Vol.29, N°1, February 2005.

Pasquet M., Vernois S., Aubry W. & Cuozzo F., (2008) "Electronic payments", *Encyclopedia of Information Science and Technology,* 2nd edition, chapter Electronic payment (212), pages 1341–1348. IDEA, 2nd edition

Reason J., (2000), "Human error: models and management", *British Medical Journal,* (BMJ) 2000, March 18th, Vol. 320, pp. 768-770

Reason J., (1997), "Managing the risks of organizational accidents", *Ashgate Publishing limited*, 243 p.

Reveilhac M. & Pasquet M., (2009), "Promising secure element alternatives in NFC architecture", Communication *IEEE International Workshop on Near Field*, 2009

Scarborough A. & Bailey L., (2005) "Examining ATC operational errors using the human factors analysis and classification system"*, Report, DOT/FAA/AM-05/25, Federal Aviation Administration*, Office of Aerospace Medicine, Washington, DC, December 2005.

Wiegmann D. A., and Shappell S. A., (2003), "Human Error Approach to Aviation Accident Analysis", *The Human Factors Analysis and Classification System*, Ashgate Press (ISBN 07546 1873 0), September 2003