Contactless Payment

Investigating the myths and realities of contactless payment fraud

July 2013 - Updated April 2016

1. Executive Summary

Contactless payment cards have been in the news for all the wrong reasons over the last few months.

Phantom and duplicated payments in some UK retailers have led to headlines asking ‘how safe is your money?’ and references to ‘controversial new payment methods’.

We’ve also seen Newcastle University's Centre for Cybercrime and Computer Security demonstrate ‘how easy it is’ to scan card details from contactless payment cards – raising fraud and cybercrime concerns.

In light of these recent stories, and the inaccuracies sometimes reported within them, the SPA published a first version of a position paper to uncover the myths and realities of contactless payment risks. Since the original publication, a dramatic increase in terms of number of contactless transactions has been observed enabling to collect fraud data to elaborate the first reliable statistics. In particular as explained in paragraph 6 below, our initial analysis explaining why we believed contactless payments were safe is backed by the first published figures on fraud levels by the Banque de France.

Added to this, we firmly believe that user education can, and should, raise public awareness of the realities of the potential security threats of contactless payment. So, by offering an analysis of contactless payment security, the paper provides an expert, independent view. It details the potential forms of attack - both real and theoretical – and highlights the countermeasures in place to respond.

Crucially, this paper will be regularly updated and made publically available to assure the highest levels of transparency, to report against potential new threats as they appear, and to chart ongoing industry activity to address and minimize risk In this respect we note that at present, in the retail payments industry “contactless payments” refer to both, payments initiated with a plastic contactless card as well as payments using a mobile device with a NFC interface, also known as “mobile contactless payments”. This second version of our report takes into consideration that fact and therefore includes new material to address new risks created by mobile contactless payments. SPA points out however that available data for contactless payments fraud relate exclusively to plastic cards.

2. Identified vulnerabilities for contactless cards

Let’s begin with what a contactless card actually is and how it works. Put simply, it is a card that integrates an antenna and a chip using a standard communications frequency of 13,56 MHz. To initiate a transaction/communication, the contactless card must be placed in close proximity to the contactless terminal – which then emits a reduced magnetic field just enough to activate the card at a distance of several centimeters (typically 1 to 4 cm/1 inch).

Contactless technology is ideal for payment cards as it enables very fast transactions (less than 500 ms - milliseconds), ease of use (the payer simply presents the card to the reader to pay) and is low cost (using standardized technology). Despite these features, the nature of the contactless channel means it can be accessed by a third party, and this may be exploited by an attacker.

However, it is important to state that there are over 300 million contactless cards in daily operation around the world. Very few incidents have so far been reported, and these have tended to involve failed transactions rather than attacks leading to actual financial losses for the cardholder. Fraud data are detailed in Paragraph 6 below.

But the payments industry is far from complacent.

It is theoretically possible to access contactless card data, as has been proved by Newcastle University and others in lab conditions. How easy it is to replicate these results in the real world, what information can be gathered, and how useful the captured data will be to fraudsters, are other questions.

Regardless of this, the SPA strongly believes in the value of such research in providing data to further reduce risk - and we are entirely supportive of similar projects going forward.

Known RF Vulnerabilities

Contactless payment cards (and mobile payments) work using Near Field Communication (NFC) technologies – by placing the card (or the handset) onto or within 4 cm of the antenna of a point of sale contactless payment terminal. The card is activated and communicates with the terminal via the Radio Frequency (RF) channel established between the card and the terminal.

There are already well known vulnerabilities within the RF interface. These can, theoretically, lead to skimming attacks, card data being captured when transmitted over the radiofrequency channel, or denial of service attacks. These attacks are detailed below in this paper.

However, SPA members have developed a major body of research and made significant investments in developing countermeasures to ensure these RF vulnerabilities cannot be easily exploited outside the RF laboratory environment.

The platform for much of this research is activity that has already been carried out by governments, homeland security agencies and the EU during the development of electronic or so-called ePassports.

While ePassport and contactless payment use cases have significant differences in application, they both share the same underlying technologies and RF interfaces. As a result, the payments industry has benefited significantly from the dramatic improvements in ePassport-to-terminal security that major public sector investments have already delivered.

However since the publication of the previous version of this report, new contactless payment vulnerabilities have been introduced by the use of the mobile device to pay. Unlike the smart card operating system, the rich operating system of the mobile device was not designed to secure resident payment data. End-users are well aware and that fact appears as a first reason for the disappointing adoption of mobile payments. Security countermeasures have therefore been developed for integration in the mobile platform to minimize threats. They are briefly described in Paragraph 5 below.

Of course, as with any form of security, systems are not infallible. Security is a compromise between delivering the highest degree of protection and offering the user the highest levels of convenience. But, as we'll see, with contactless security now a mature field, and having been engineered to make fraud economically unfeasible, actual real-world risks are minimal.

3. A Secure RF History

The first mainstream RF device to receive a comprehensive analysis of security vulnerabilities was the ePassport. In common with contactless payment today, a number of studies were published that pointed to potential areas for concern.

These ranged from the design of the personal data transfer via the RF interface to the security embedded within the ePassport. Also outlined were the risks of fake or duplicate passports being produced to acceptable standards by criminal and terrorist organizations.

In response to these papers, and recommendations from their own advisors, governments and public bodies across the world, including the European Commission, funded multiple initiatives to better assess the risk profile. These activities, alongside a series of bid-test programs, delivered dramatic security improvements in the ePassport-to-terminal RF interface.

The resulting solution saw embedded ePassport chips combine the capacity to store certificates and biometric references with high levels of durability and interoperability. Ultimately, the work provided a catalyst for an extended range of contactless services – and provided the foundation for today's generation of contactless cards, mobile devices and RF payment tags.

The following sections describe these potential card and mobile vulnerabilities, analyze real-world risks and discuss the countermeasures implemented within the contactless card environment to mitigate fraud.

4. Analyzing RF Vulnerabilities

Let's first look at the vulnerabilities of the RF interface. As we have seen, there are known vulnerabilities inherent in the RF interface when a contactless card, which may or may not be a payment card, is activated and communicates with a contactless terminal.

It should be noted that some of the assertions hereafter do not apply when the card is embedded in a mobile device as a Secure Element for a NFC payment. This issue is addressed in the next paragraph.

Compared with contact cards, when deploying a RF secure device, the following risks, as described in Table One below, need to be addressed. Most of these threats relate to reading the information on the contactless chip without knowledge of the cardholder.

A contactless card accepts a transaction whenever a terminal activates the card without the need for the cardholder to enter data. The challenge comes because the card does not know whether the terminal is legitimate or rogue. If it is the latter, a skimming attack can occur.

Such an attack is characterized by a rogue terminal establishing a communication channel with a legitimate contactless card, then retrieving card information without the cardholder being aware.

A simple way to eliminate the risk of skimming is for the contactless card to first identify the reader trying to establish a communication with it, before sending out any information. This is the solution adopted for the electronic passport.

Unfortunately, such a safeguard is unrealistic for contactless payment cards for two reasons:

1. Payment cards, either contactless or contact, do not authenticate the terminal. Introducing terminal authentication means replacing all the payment terminals across the world.
2. Contactless payment is predicated on speed – for example, reducing queuing time at the store. Terminal authentication will add a significant time delay to the transaction – eliminating any real value in using contactless cards to make payments.

Table One summarizes the latest information on the known vulnerabilities, attack patterns and financial risks. It also highlights the available safeguards that SPA members are implementing in their contactless payment products to reduce risk.

Table One: RF Vulnerabilities, Attack Patterns, Financial Risk & Countermeasures

VULNERABILITY	ATTACK PATTERN	FINANCIAL RISK	COUNTERMEASURE
A legitimate contactless payment transaction can be captured using a clandestine antenna.	'Passive Eavesdropping: A single spy-reader is placed in close proximity to the card, passively reading the data exchanged during the transaction. This attack is difficult to detect as the spy-reader simply listens and records the data exchanged. This information can be used to clone a card.	Card account data leakage could be exploited to manufacture a fake card or a clone.	Encrypting the data exchanged between the card and the reader. To authenticate contactless card to detect a cloned card.
A contactless card responds automatically (without the need for user input) when the card detects a standard magnetic field at 13,56 MHz.	'Clandestine scanning' or 'electronic pick pocket' or 'skimming'. These all refer to the same type of attack. A contactless card carried in the pocket will respond automatically when activated by a clandestine reader. This allows for the possibility of users unknowingly using their contactless card while carried in a bag or wallet.	Retrieval of card data to facilitate later card clones. Generation of a payment order signed by the card for the benefit of the attacker.	Authenticate the reader via a questioning process initiated by the card prior to any data release - with a limited number of trials before the card blocks itself. Carry the card in a metallic box acting as a Faraday cage. The card is only taken out when it is time to pay. Systematic online authorization. Deactivate the NFC interface in a mobile device, and reactivate it just when paying
	'Replay Attack'. A transaction is executed with a legitimate card via skimming, using a pre-determined challenge chosen by the attacker. The card's responses to these challenges are recorded in a fake card to be used afterwards.	Unauthorized cash withdrawal in certain categories of ATM. These ATM generate predictable random numbers which can be recorded by a fake card prior to the actual attack	Deploy 'safe' ATMs with good quality random number generators that are unpredictable.

A contactless terminal is unable to identify it has authenticated a remote chip instead of the presented chip.	'Grandmaster Chess attack' or 'Relay Attack'. These are a man-in-the-middle attacks where a fake card is presented to an authentic reader. The queries from the reader are relayed by the fake card to a fake reader - which then skims an authentic contactless card nearby. The data from the skimmed authentic card is then relayed back as if generated by the fake card. This threat is considered more serious with a mobile device	Unauthorized payment.	Relay attacks require extra-time. A system design binding the transaction time (max time authorized for a card response before payment cancellation) is a good solution.
A contactless reader will simultaneously activate all the contactless cards present in the volume (or area) of operation – generating a 'collision' and making responses unreadable.	'Denial of Service attack (DoS)'. An attacker uses a rogue reader to saturate an area (e.g., a store) by activating multiple contactless cards. This blocks any individual payment transactions.	A DoS attack may simultaneously target multiple communications, thereby rendering the transaction impossible. While the impact of a DoS attack can be significant for consumers and merchants for the duration of the attack, there are no potential fraud issues - either in real-time or in the future. Financial or personal data cannot be collected, and with the lack of financial gain for the attacker, such threats are not considered to be serious.	For normal operation, with no attacks, the implementation of anti-collision protocols solves the problem. ISO 14443 standardizes two of them – although EMVCo does not use them. In the attack scenario, when a rogue reader emits strong magnetic fields to saturate all the present cards, little can be done.

Low cost contactless cards have limited computational power and execute lighter cryptographic mechanisms.	'Force brute attack'. allows the payment related data to be read after the transaction is recorded.	If the transaction is decrypted the attacker has succeeded in eavesdropping the transaction – which can lead to card cloning.	Lightweight cryptographics has been standardized to provide an optimized trade-off between performance and a level of security proportionate to the risks of typically low value contactless payments.
The transaction is performed without cardholder verification (No PIN code required).	'Impersonation'. Should a contactless card not support PIN verification, it is entirely possible for lost or stolen cards to be used by someone other than the legitimate cardholder – as payment authorization is simply granted by placing the contactless card in front of the terminal.	Unauthorized payment transactions will continue until the card is revoked.	Include a Cardholder Verification Methodology that protects the user if the card is lost or stolen. For instance MasterCard products are using either Signature or Online PIN over the contactless interface In a mobile device, a mobile code and/or biometrics may be used to verify the presence of the legitimate user.

Threat Summary (from Table One)

- It should be noted that the specific RF channel and cost constraints may lead to a higher probability of failed communication that may be exploited by fraudsters.
- Details of the complex, combination attacks (as we see above) have been widely published. SPA members are well aware of research in these areas and have designed efficient safeguards to minimize risk.
- The threat offered by both skimming and eavesdropping attacks relate to the potential capture of card data. This can be used in real time to create a 'real-false' transaction (relay attack), to impersonate the user (in an internet payment) or to produce fake cards.
- Despite the potential for attack, the very same technical limitations of the RF interface actually helps prevent misuse: the limited energy involved, low transmission range, simple modes of communication, vulnerability to noise and so on.

This technical rationale is backed by the first reliable statistics on payment contactless fraud published in 2015 by the Banque de France. See below in Paragraph 6.

5. Identified Vulnerabilities of mobile contactless payments

From the functional point of view, a mobile contactless payment performs the same way than a contactless payment card. Therefore the vulnerabilities over the radiofrequency interface are the same when payment data are in transit. The mobile device however presents the advantage that the NFC interface can be deactivated, and be only reactivated at the time to pay. With this functionality the payment credentials cannot be skimmed when they are at rest. It is also true that the loss of a mobile device is usually noticed faster than the loss of a payment card. This fact is likely to reduce the observed prevalent fraud patterns for contactless cards which tend to be misused when lost or stolen. But next to these recognized advantages, the security for mobile contactless payments is challenging because of the intrinsic vulnerabilities of the mobile operating system. These vulnerabilities bring about that hackers keep the mobile security controls on the spot.

Mobile devices feature four additional vulnerabilities compared with contactless cards:

1. It's easy to download malware taking the control of the mobile operating system
2. The user often increases the threats for payment applications by jailbreaking it
3. Multiple communication channels that are potential attack points especially considering that the mobile is often permanently connected (but the NFC interface may be deactivated)
4. Pure software implementations for data and applications (Host Card Emulation - HCE) executed directly by the mobile operating system which are insufficiently proven.

These vulnerabilities translate into threats for the payment applications that can be categorized as

1. Threats to mobile contactless payment applications (key extraction, code breaking, credentials stolen)
2. Threats for transactional data in transit, similar to those for the contactless cards, with the exception that relay attacks are thought to be easier with a mobile device (malware installed in the victim mobile and remotely activated)
3. Disruptive attacks which may be prompted by installed malware (Denial of service, that in case of the contactless card requires a rogue terminal

SPA considers that the best countermeasure against these threats consist in the implementation of a certified hardware isolated environment for the storage and execution of payment applications and data. In order to further protect the user, a trusted user interface enabling the entrance of personal verification data (mobile code, biometrics) is highly recommended. Both security countermeasures will facilitate the compliance with strong customer authentication requirements. In that case, mobile contactless payments above the legal threshold (above 20 euros for instance) for a contactless card payment with no CVM.

If for market reasons, pure software implementations are requested, then additional countermeasures are needed: white-box cryptography, tokenization and/or storage of long-term credentials in the cloud.

6. What the fraud statistics say

The current substantial experience in terms of number of transactions means that for the first time the industry benefits from reliable statistics data specific to contactless payments. Thus, the Observatoire sur la Fraude Carte of Banque de France in its 2015 report presents a level of fraud for contactless transactions of 0,015% corresponding to the data recorded along 2014. For comparison purposes, the level of fraud for contact transactions is established at 0,010% and it's less than a half of the fraud observed for cash withdrawal operations in ATMs estimated at 0,034%.

For SPA it is important to outline that the fraud on contactless transactions is originated from contactless cards stolen or lost, not from their normal operation by the legitimate user. These data comfort our initial security analysis published in 2013 concluding that payments with contactless cards were safe. These data are likely to change with the increasing adoption of mobile payments, especially if for commercial reasons, the use of less secure technologies is privileged. But at present, no serious statistics by a recognized organization are available with respect to the observed level of fraud for mobile contactless payments. SPA will be updating the present report and providing with the corresponding analysis when new figures related to contactless card fraud or the first data corresponding to mobile contactless payment fraud will be made available.

7. Moving forward: Managing Fraud

SPA members are engaged in ongoing work with stakeholders across the card payments industry - EMVCo, SEPA-European Payments Council, National Regulatory Authorities and the Eurosystem - to identify emerging attacks and implement security safeguards in their products.

The only successful attacks to have been documented have been carried out by academic institutions during specific research programs (and in lab conditions). These have helped card vendors and issuers redesign countermeasures, and support continuous improvement programs.

The security policies to tackle fraud are defined by the issuer and the merchant acquirer banks following guidelines specified by the payment schemes. They address the mechanisms for card authentication and cardholder verification methodologies to fight against counterfeit and fraudulent transactions, including:

- Counterfeit transactions performed with a fake contactless card
- Fraudulent transactions performed with a legitimate contactless card but not by the genuine user to whom the card was issued
- Fraudulent transactions generated by malware installed in the mobile device operating system

The choice of the most appropriate combination of card authentication/cardholder verification will depend on the type of contactless payment application being stored in the card.

8. Conclusions

It is the SPA's belief that better, more accurate information on the real-world risks involved in contactless transactions is needed, especially when they are initiated by a mobile device. More knowledge and greater transparency will facilitate adoption by addressing many of the security myths that are circulating today.

For our part, the SPA is willing to collaborate with issuers and operators in order to:

- Increase awareness of information security threats connected with contactless and mobile contactless payments and simple ways to overcome them
- Orientate the choice of security mechanisms, including modern and well proven cryptographic protocols and algorithms adapted to both contactless cards and NFC mobile portable devices
- Provide the industry with a detailed methodology to evaluate risks
- Provide insight in the requirements and practical aspects for the implementation of data protection and anti-money laundering legislation
- Facilitate effective security management practices for the operation of contactless and mobile contactless payments.

Regardless of the more sensationalist headlines and the security holes inherent in the RF interface, the reality of a contactless deployment is thousands of hours of an extensive and rigorous security evaluation by independent, accredited laboratories.

During these evaluations, the resistance of the contactless cards to a host of differing attacks from the most advanced technologies is fully tested. The output is a security evaluation report, detailing all identified strengths and weaknesses before the solution is certificated and distributed.

But the SPA is committed to remaining alert, and working proactively to assure security remains high. Going forward, as new threats emerge, the payments industry will continue to respond, and the SPA will continue to chart developments of both challenge and solution – separating myth from reality.