10.20378/irb-58524

Risk Analysis of NFC Payment Systems

Jonathan Reimers

Academy of Hamburg Police, Carl-Cohn-Straße 39, 22297 Hamburg,
jonathan.reimers@polizei.hamburg.de

Prof. Dr. Wilfried Honekamp

Academy of Hamburg Police, Carl-Cohn-Straße 39, 22297 Hamburg
wilfried.honekamp@polizei-studium.org

Abstract:

This chapter examines the question of whether manipulation of near-field communication (NFC) payment systems is possible, whether existing security measures adequately protect this technology, and to what extent criminality in this area has already progressed. As IT penetrates more and more areas of everyday life, this inevitably leads to new risks and dangers. This, in turn, poses new challenges to law enforcement agencies, as any specialized IT crime has to be readjusted. Initial experimental studies have already identified security risks in NFC technology. However, there are many more potential risks to check. Based on an experiment, it was examined to what extent the interception of credit cards via NFC with a standard smartphone is possible. Afterwards it was examined whether with the obtained data goods could be ordered and paid in different Internet shops. As a result, it becomes clear that reading out the credit card data by means of the NFC function of a commercially available smartphone is possible and, depending on the respective carrying situation, promises a high probability of success.

JEL Classification: O33, K39

Keywords: Near-field communication, NFC, experiment, information technology, interception, credit card, credentials.

1 Introduction

The developments in information technology make many aspects of everyday life easier and faster. In addition to innovations in communication, locomotion and computer technology, even the advanced use of credit cards, payment transactions can be done as quickly as possible. There is a need to be able to make payments faster and more convenient and the costly cash flow is increasingly avoided. In 2017, 46.9% of payments were made without cash and this value tends to increase (Rüter 2018: p.9).

In 2002, the technology near-field communication (NFC) was developed, which makes it possible to complete the process at payment terminals by simply placing a credit card with NFC chip. Since its launch in 2002, the use and relevance of NFC technology has grown steadily. Looking at Mastercards NFC program Paypass as an example, only 20 million Paypass credit cards were accepted in 2007, which were accepted by 80,000 companies. As early as the beginning of 2011, the number of Paypass credit cards had increased to 92 million, which are accepted by 311,000 companies (Mastercard 2011: p. 1 & 5).

However, in addition to this growing relevance for NFC technology, there is also an increased risk of becoming a victim of crime. There are still security holes that can be exploited by specialized criminals. The present work will deal with the existing possibilities of abuse and the processing of one of the most likely forms of intervention. Thus, the greatest risk is that the data of a credit card are transferred via NFC chip, as it is the easiest way to realize the attack and has the lowest risk of discovery. Thus, an attempt is being made to find an answer to the question of whether it is possible to intercept NFC credit card data and use them illegally. This work will focus on an approach that would be feasible for less specialized offenders. Consequently, only means are used that are free and legally available to everyone. Findings regarding spy probabilities are to be obtained through experiments conducted in different constellations. Subsequently, the possibility of further use of the obtained data, e.g. by the purchase of goods on the Internet, is to be examined.

Finally, an answer is given on whether NFC technology will provide a basis for further criminal action, or whether there are enough security mechanisms to prevent any action. It is also important to find out whether the police are already warning of the potentially existing security risks of NFC technology in order to combat possible crime.

2 Material and Method

To scientifically test a practical use of NFC systems by perpetrators, the question “Is it possible to listen to NFC credit card data and to use this data illegally?” is to be

checked. To answer the question scientifically, experiments are used. Since the research question aims at a practical application by criminals, this should also be answered by practically applied experiments.

Starting with listening to the required data, both the required distance, in which the active-mode switched NFC module must be located, so that the data is still transmitted, and the read-out probability are discussed. To ensure a close-to-life uniformity, different wearing situations were simulated, which are common in everyday life. The structure of the individual experiment runs is explained in more detail below.

Figure 1: Left – card in a jeans pocket (1, 2) and right – in an outer pocket of a polyester jacket (3)

Experiment (1) – the credit card is in a genuine leather purse measuring 10.5 cm x 11.5 cm. The card is inside two layers of leather and two layers of fabric. The leather wallet is empty in the experiment. The leather wallet is in a jeans pocket.

Experiment (2) – the credit card is in a genuine leather purse measuring 10.5 cm x 11.5 cm. The card is inside two layers of leather and two layers of fabric. The leather purse contains 8 x € 0.50 coins in the coin compartment and three cash notes in the cash drawer compartment. The card slots contain two NFC-incompetent cards. The leather wallet is in a jeans pocket.

Experiment (3) – the credit card is in a genuine leather wallet measuring 10.5 cm x 11.5 cm. The card is inside two layers of leather and two layers of fabric. The leather wallet is empty in the experiment. The leather wallet is in the outer pocket of a polyester jacket.

Experiment (4) – the credit card is in a genuine leather wallet measuring 10.5 cm x 11.5 cm. The card is inside two layers of leather and two layers of fabric. The leather wallet is empty in the experiment. The leather purse is located in the outside pocket of a leather handbag.

Figure 2: Left – card in the outside pocket of a leather handbag (4)
and right – in the outside pocket of a backpack (5)

Experiment (5) – the credit card is in a genuine leather purse measuring 10.5 cm x 11.5 cm. The card is inside two layers of leather and two layers of fabric. The leather wallet is empty in the experiment. The leather wallet is in the outside pocket of a backpack.

Experiment (6) – the credit card is in a genuine leather purse measuring 10.5 cm x 11.5 cm. The card is inside two layers of leather and two layers of fabric. The credit card is in a professional RFID block box. The leather wallet is empty in the experiment. The leather wallet is in a jeans pocket.

Experiment (7) – the credit card is in a genuine leather purse measuring 10.5 cm x 11.5 cm. The card is inside two layers of leather and two layers of fabric. The credit card is wrapped in a simple, self-made aluminium foil sheath. The leather wallet is empty in the experiment. The leather wallet is in a jeans pocket.

Figure 3: Left – an RFID block box (6) and right – an aluminium foil sheath (7)

The experiments are carried out as follows: The smartphone is activated with enabled NFC function and the Scanless App Contactless Credit Card Reader from MaxSoft

Ltd. held against the object for two seconds (e.g. the jeans or jacket pocket). If the credit card data are read, the test result is considered a success, if not, as a failure. For each of the seven experiments 100 test runs are made. The tests are carried out with an NFC-enabled smartphone (Samsung Galaxy S7) without a cell phone case, which any potential culprit can acquire. After transferring the data, tests will show whether they are sufficient to order and pay for goods on the Internet.

3 Results

The results of intercepting the NFC signals and using the obtained data are presented below. The experiments showed that readout of the data by a simple smartphone requires a direct application to the object. If the smartphone is not on, the distance is already too large and the data cannot be received. As can be seen in table 1, different success probabilities were measurable for each of the 100 experiments in different experimental constellations.

No.	Design	Success	Failure	Probability
(1)	NFC-enabled card in empty leather wallet in jeans pocket	84	16	**84 %**
(2)	As experiment (1), but + 2 NFC-incompetent cards + 8 x 50 cents coins + 3 cash bills	76	24	**76 %**
(3)	As experiment (1), but in a jacket pocket	80	20	**80 %**
(4)	As experiment (1), but in leather handbag	23	77	**23 %**
(5)	As experiment (1), but in backpack	78	22	**78 %**
(6)	As experiment (1), but NFC-enabled card in RFID block box	0	100	**0 %**
(7)	As experiment (1), however, NFC-enabled card wrapped with aluminium foil	0	100	**0 %**

Table 1: Results of the experiments

In Experiment (1), the NFC-enabled credit card was in a leather purse in a denim pocket. With 84 successful attempts and 16 failures, the probability of success was thus 84%. Experiment (2) had in addition to the NFC credit card still 2 NFC-incompetent cards, and 8 x 50 cents coins and 3 cash notes in the leather wallet. In 76 successful trials and 24 failures, the probability of success was 76%. Experiment (3) differed from experiment (1) only in that the leather wallet was in a polyester jacket pocket. With 80 successful trials and 20 failures, the probability of success was 80%. Experiment (4) with the placement in a leather handbag resulted in 23 successful attempts and 77 failures – this corresponds to a probability of success of 23%. In experiment (5) a backpack was used. The results showed 78 successful trials and 22

failures. Thus, the probability of success is 78%. In Experiments (6) and (7), as in Experiment (1), the NFC-enabled credit cards were in a leather purse in a denim pocket but were still in Experiment (6) in an RFID block box, as well as in Experiment (7) enclosed in an aluminium foil wrapping. Both experiments (6) and (7) yielded 0 successful trials and 100 failures. Thus, the probability of success was 0% each.

In the experiment, it was also noticed that the probability of success depended strongly on the correct positioning of the smartphone, since the NFC antenna of the smartphone must be brought as close as possible to the NFC-enabled credit card. The optimal positioning is shown in figure 4.

Figure 4: Device Design Samsung Galaxy S7 (Samsung Electronics 2016: p. 7)

If the readout is successful, the app will display both the card number and the expiration date of the credit card, as shown in figure 5.

With the obtained data we now try to order and pay at various Internet shops. However, as shown in figure 6 for example, IKEA asked in addition for the three-digit security code, which is printed on the back of the credit card and is not sent via NFC transmission. An order with these dealers is therefore not possible.

However, this is different with Germany's largest online retailer Amazon (Hofacker, Langenberg, Langer 2019). Amazon does not ask for a three-digit security code, but asks for the name of the cardholder. This is also not transmitted when reading NFC data. If you enter an obviously fictitious name as Max Mustermann, Amazon shows an error message and cancels the ordering process.

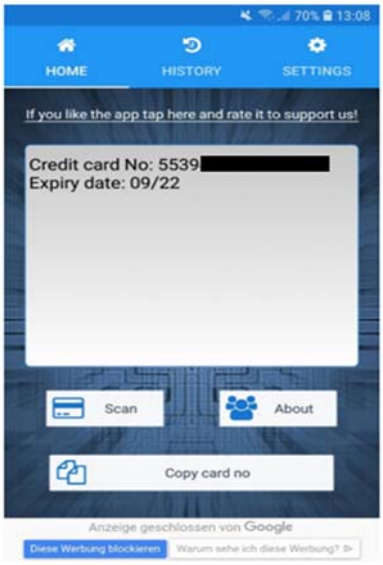

Figure 5: Screenshot of a successful readout with the app Credit Card Reader

Figure 6: Terms of payment at ikea.de

However, if, as shown in figure 7, a name common in Germany but not the same as that of the credit card holder is given, Amazon accepts the payment and allows the buyer to send the goods to any address. This does not have to contain the same name as stated in the payment information.

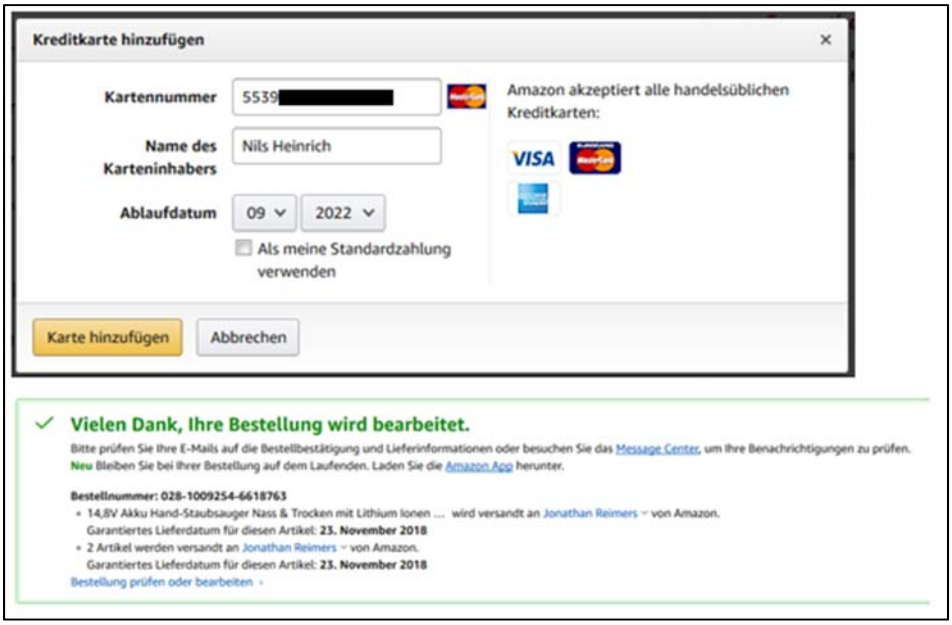

Figure 7: Successful order at amazon.de with spied out data

4 Discussion and Conclusion

The research question “Is it possible to listen to NFC credit card data and its tortuous use?” was answered by the experiments carried out. The experiments prove that it is already possible with freely accessible means such as smartphones and free apps to read the data from credit cards, even if they are inside a purse in a pocket or jacket pocket. Although not every selection attempt was successful, the probability of success was so high at approximately 76%–84% that several readout attempts would quickly lead to a large data pool. It can be assumed that the probability of success can be further increased with soaring practice.

Experiment 4 differs with only 23% successful readouts to the comparatively high probability of success of the other experiments. Since the placement of the purse in a leather handbag was harder to locate, reading out became more problematic. This makes it clear that placing the NFC-enabled credit card in larger containers, in which the positioning of the card is harder to assess, reduces the risk of eavesdropping. It was also found that it is not without problems to use the data obtained to order goods. Most online retailers require payment of the three-digit security code, which is not read out, but a wide range of possible online retailers is not necessary because, for example, Amazon only asks for the credit card holder instead of the security code and this is not checked internally. So each offender can think of any name and order freely with the obtained data. In the assortment of Amazon there are enough high-quality products which could easily be ordered in large quantities and resold, e.g. expensive smartphones, cameras or jewellery.

In order to compensate for the lack of security mechanisms of NFC technology, it is advisable for the user to take precautionary measures to avoid becoming a victim of an NFC-related crime. The credit cards should be in an RFID block box or aluminium foil box. Experiments 6 and 7 proved that this effectively prevents readout of the data by means of NFC. As an added security measure, users should store their NFC-enabled credit cards in larger containers rather than in their pockets. As the distance to the listening module is slightly increased, the likelihood of a successful listening attack decreases (see experiment 4). In general, a more conscious appearance in busy places (such as in public transport or shopping centres) is helpful, since an approach can be detected by potential perpetrators so early. In order to detect an unnoticed interception and to take measures as quickly as possible, such as an account lockout, it is advisable to check the account statements regularly and to look for unauthorized debits. If the NFC function of the credit card is not used, it is possible to switch it off at the bank to be issued.

Although other experiments have already shown that it is possible to read the data from an NFC-enabled device, the findings of the present work are valuable in that they demonstrate the ability to read out with simple means and in real-life situations. The subsequent use of the obtained data was not described in detail before. These two findings make it clear that there is only a relatively small risk of detection for offenders to intercept the NFC data and then use it unlawfully. This assessment should be of particular value to police authorities.

The NFC technology also offers – in addition to the examined credit card payment systems – the function to transfer data via a smartphone and even make payments. From mid-2012 to 2018, the number of smartphone users in Germany rose from 27.3 million to 57 million (Statista 2019a). This trend can also be observed globally. The number of smartphone users worldwide rose from 1.06 billion to 2.6 billion by 2018 (Statista 2019b). In particular, the growing number of smartphone owners suggests that NFC technology could be a target for criminals through this medium as well. Closer investigation in this area may also be of interest to police authorities. This work focuses on reading the data through simple means such as smartphones and free apps. However, the data can also be read out in other ways. There are e.g. NFC card readers that send the data via Universal Serial Bus to a connected computer or laptop. A review of whether the use of such funds would increase the probability of eligibility could contribute to the overall understanding of NFC safety.

However, the methodology used in this work also had limitations. Thus, the experiments could be extended to allow a more accurate statement regarding the readout probability. On the one hand, different smartphone models can be used to show whether transmission powers of different strengths exist, as well as other carrying

situations, such as e.g. other purses or different fabrics of the jacket or trouser pockets. Also, different apps could be used to check whether there is a connection between the probability of reading and the app used. Furthermore, the number of tests carried out can be further increased in order to achieve an even more accurate result. The examined use of the obtained data also contained several limitations. A purchase attempt could be carried out only at a limited number of online shops. Further attempts could possibly show more purchase possibilities than only Amazon. Also, the experiments used in purchases remained in the online trade. Subsequent experiments could deal with other ways to use the obtained data. For example, it is possible to pass on the credit card details by phone during a hotel booking and to order laptops for a meeting scheduled there. These could then be stolen and sold. Also for this application, the obtained NFC data may be sufficient.

The experiments used in the present work show that it is possible to read the credit card data by means of NFC through a smartphone and to use the obtained data on the Internet to purchase goods with little effort. It does not require any special expertise by the offender, as no exact understanding of the NFC technology is needed to obtain the data of the credit cards. Also, the acquisition of the means of action poses a potential culprit with no high challenges, since both a smartphone, as well as the required app are available legally and inexpensively.

If the next step is to ask about the security mechanisms used, it must be concluded that, apart from the required range, the NFC technology hardly uses any mechanisms to increase security, thus making the data available unencrypted to potential devices in the environment. In particular, if in the future specialized offenders should resort to using devices that increase the read range, they could read large amounts of data in a short period of time without incurring a discovery risk. A modernization of the technology, in which the data is transmitted only encrypted, would be urgently needed at the latest.

Even if the security situation of NFC technology draws a bleak picture, a rapid spread of NFC-related crime in the near future is not very likely. In addition to the possible undiscovered cases, the actual reported offenses in Europe are currently at a very low level and the knowledge of the opportunities and risks of NFC are generally not yet widespread. However, should the use of this technology continue to increase, the risk of criminal misuse also increases.

In order to warn of the risks of NFC technology, law enforcement authorities in particular should provide preventive information. The experiment has shown that even simple security measures can significantly reduce the probability of success of perpetrators. Hamburg police does not carry out at the moment, however, any prevention campaigns concerning the NFC risks. In view of the rapidly growing IT areas and the

ever-new technologies, however, it is difficult to be warned of any new risk. However, if the case numbers in the field of NFC-related crime increase in the future, an awareness-raising campaign with protection notices, such the use of RFID block boxes, would be essential.

5 References

Hofacker, L.; Langenberg, C.; Langer, N. (2019): E-Commerce-Markt Deutschland 2019. Accessed on 13.10.2019 at https://www.ehi.org/de/top-100-umsatzstaerkste-onlineshops-in-deutschland

Mastercard (2011): Paypass Momentum. Accessed on 13.10.2019 at https://newsroom.mastercard.com/wp-content/uploads/2011/09/MasterCard-PayPass-Momentum-May-2011.pdf

Rüter, H (2018): EHI-Studie – Kartengestützte Zahlungssysteme im Einzelhandel 2018, Köln. Accessed on 13.10.2019 at https://www.ehi-shop.de/image/data/PDF_Leseproben/EHI_Studie-kartenges_Zahlungssysteme_2018_Leseprobe.pdf

Samsung Electronics (2016): SM-G930F Benutzerhandbuch. German. 02/2016. Rev.1.0. Accessed on 13.10.2019 at http://downloadcenter.samsung.com/content/UM/201602/20160222105002581/SM-G930F_UM_Open_Marshmallow_Ger_Rev.1.0_160219.pdf

Statista (2019a): Anzahl der Nutzer von Smartphones in Deutschland in den Jahren 2009 bis 2018. Accessed on 13.10.2019 at https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

Statista (2019b): Prognose zur Anzahl der Smartphone-Nutzer weltweit von 2016 bis 2021. Accessed on 13.10.2019 at https://de.statista.com/statistik/daten/studie/309656/umfrage/prognose-zur-anzahl-der-smartphone-nutzer-weltweit/