Haaga-Helia
University of Applied Sciences

NFC Payment & Security Threats

Niko Korhonen

Bachelor's Thesis
Degree Programme in
Business Information
Technology
2017

Haaga-Helia
University of Applied Sciences

Abstract

Author(s)
Niko Korhonen

Degree programme
Business Information Technology

Report/thesis title
NFC Payment & Security Threats

Number of pages and appendix pages
38 + 6

This thesis goes through the known methods of NFC utilising contactless payment and the security issues and threats of each specific device or method. The thesis will cover the known in use devices in Finland and the methods for each device. The technology and origins of NFC is also explained in detail, as well as the protocols standards and Android development tools constantly keeping in focus the aspects that affect security. The thesis also includes two researches and the goal of the thesis is to map the security threats there are in NFC utilising contactless payment.

This thesis is conducted without a financial supporter, but the results will be forwarded to any party that might benefit from the results of the research.

The thesis does not handle or analyse any other forms of contactless payment other than those that utilise NFC technology. This means that even though some applications i.e. Mobile Pay are mentioned, they are not analysed or taken in count when defining the results of the research.

The sources and materials used in this thesis consists of previous studies, tests and articles, technology and component descriptions, a survey conducted via internet survey platform and personal tests and reports. Unfortunately, no reliable book source on the subject is available (for the information is either expired or irrelevant for this thesis). I have also used statements of bank personnel and representatives that have commented on NFC security issues during the last few years.

Research indicated that are some serious security threats in contactless payment methods that are not that well known for the public and for banks. There might be a possibility that some risks are known by banks and card companies but are chosen to be left uncommented for there are no easy answers. It was also found out that even though your “ordinary user” is not aware of the specific threats and factors, contactless payment is still not thought of as a 100% safe option but rather a concerningly unsecure one. The comments from bank representatives also revealed little about the safety aspect knowledge of the banks.

For the question, what can be done to prevent falling a victim to the explained attack scenarios in this thesis I found out some answers, but most of the results depend on either personal awareness or physical protection. The application side, as in any type of IT-security is hard to develop because the faster development of exploitation schemes in correlation to security solutions.

Keywords
NFC, Contactless Payment, IT-Security, Mobile Pay, Android

Table of contents

1 Introduction

In my thesis about NFC payment and security threats I will go through the basic technology and devices that are used in NFC payment and the known forms of security risks. The thesis was conducted single handedly by me, meaning that there were no sponsors involved. As for the objectives of the thesis I set out to research what is the current state of security in paying with NFC in Finland and in some parts the world and also what is the overall stance towards the security of NFC payment of the average end user. I also set an alternative or additional objective depending of the results to: what can be done to enhance the security of NFC Payment? As for the research problem of my thesis I altered it once again depending on the results but with the assumption that there are some serious risks in NFC security. The research problem could be described as: how safe is NFC payment and how aware are people and bank representatives about them? Which I then started to unravel using quantitative survey analysis and case studies and interviews. The research problems in my thesis were the rapidly outdating information and in some aspects bank secrecy agreements.

The thesis starts with descriptions of all devices that are NFC paying enabled such as bank cards and mobile phones. Then the technology and the origins of NFC is explained in detail with the full descriptions of the NFC modes and protocols and standards. I also go through some of the main features in the NCI android development stack to give the reader awareness of the android technology before I go through some attack scenarios that have the android stack playing the main role. Once the technology is thoroughly explained the thesis will cover all the most known attack methods and security threats, siting results from previous tests and studies as we go and offering visual aid to understand the course of each attack and what needs to have happened in what order for each attack to be successful from the attacker’s perspective. This covers the theory part of the thesis, then we move on to the research.

In the research part I have a walkthrough of a survey I conducted which aimed to map how ordinary users of NFC payment feel about the security aspects of it. After analysing the results, I aimed to explain the results through careful assessment of various news stories in the past few years, the comments and publishes of security professionals, the comments and publishes of officials such as VISA and bank representatives and my own experiences and tests. Three cases are then gone through to support the claims and results.

In addition to the survey research I also interviewed a few colleagues of mine from Nordea bank, some in the developing process of the NFC technology utilizing mobile phone application Nordea Pay and some as a part of the survey research. Bank secrecy agreement restrained the technical analysis of the application but the discussions were supportive to my research and offered the most up to date opinions from an expert in my thesis. I conclude the thesis with a recap of the findings and ponder upon the future of NFC payment in Finland.

1.1 Terminology

The most used terms explained, to help the reader understand what the subject is:

- NFC = Near Field Communication, a determined set of communication protocols that utilize RFID technology. NFC is its own technology as well.
- RFID = Radio Frequency Identification, the technology invented in the 80's from which NFC is built from.
- NFC Tag = A smart chip that allows reading and or writing via NFC.
- NFC Antenna = A NFC utilising circuit built in a device, works like a chip with some alterations.
- NFC Mode = Devices and tags can have 3 different modes, like read/write, emulation etc. a mode defines what the NFC device does.
- Contactless Payment = A payment method that uses NFC technology
- POS = Point of Sale, a device that charges a NFC payment device
- Bluetooth = a wireless technology standard for exchanging data.
- Wi-Fi = Technology for wireless local area networking with devices
- GRPS = A digital mobile telephone technology that allows data transmission
- EDGE = Same as above, but with enhancements in speed and performance
- PCD = Proximity Coupling Device, can be an any NFC enabled device such as a smart phone
- PICC = Proximity Integrated Circuit Cards is usually a NFC tag or a sticker.
- NFC Forum = A non-profit organisation dedicated to developing NFC technology and Standards.
- Protocol = A special set of rules and end points
- Standard = a special set of protocols and communication methods and technology set as standard.

All other and some of these terms are explained in detail in the rest of the thesis text. All terms are also explained in a chronical order so that no term is explained after an example, but always beforehand.

2 Contactless Payment Devices

Contactless payments are made possible with NFC. NFC or Near Field Communication is a determined set of communication protocols that utilizes RFID technology to verify the connection between two devices. Usually the other device being a mobile phone or a bank card and the other device a stationary reader of sorts. The term “contactless payment” is used in several different instances so in this chapter I will go through the most known and most widely used devices in Finland that use contactless payment.

2.1 Bank cards

Probably the most common and everyday device that uses NFC as a payment method is the average debit or credit card. Most Finnish banks offer their customers a chance to add the contactless payment feature to his or hers card of choice and pay small shopping’s with the card. The obvious advantage of the contactless payment method in bank cards is that the end user does not have to type in the pin code when the overall sum of the purchase is under 25€. (Nordea 2017).

All the cards and the devices that support contactless payment have the signature logo on them, that is formed of 4 curved waves as such:

(Figure 1. The contactless payment logo, dynatracker.de 2016)

The contactless payment is at the moment available only for debit or credit cards that are not partnership cards such as Stockmann MasterCard or Finnair MasterCard, although they might become available soon as well. Also, the Visa Electron card does not support contactless payment technology because of its instant verifying technology. (Nordea 2017).

(Figures 2 & 3. Contactless Payments with the two most commonly used readers in Finland. Sv-oy & lansi-savo 2016)

2.1.1 The Card Types

- Debit card – A debit card is a payment card that charges the sum of the users purchases straight from the user's bank account. Debit cards do not have a credit option. The charging of the user's bank account does not happen instantly and there might be a 1 to 3-day delay between the purchase and the charge from the account so it is practically possible for a debit card user to exceed the limit on the bank account which results in the balance being negative.

- Credit card – A credit card is a payment card that does not charge the customers bank account but the credit account that the bank of the customer has granted. Usual credit providers are Master Card, Visa, Amex etc. so the credit risk of the bank is minimal. In most common cases the customer has a 30-day payment time without interest on the purchases made via credit cards, but the credit account has its own expenses such as: the banks own marginal interest added to a 3- 12 month euribor interest, service fees and the invoicing fees. Credit card users can pay their used limit in parts (usually min. 5% of used total) but the owners of payment time cards must pay the entire used sum after the 30-day interest fee period.

- Electron card – As mentioned earlier the electron card is much like the debit card in the fashion that it charges the purchases from the user's bank account. The only and the major difference is that the electron card requires an internet connection to work properly because there is no delay between the purchase and the charging.

- Credit/Debit card – A credit/debit card is the combination of Debit and Credit cards. It possesses the features of both cards in one. When paying with a credit/debit card the user chooses which side to use before entering the pin code. As a default setting when using a combination card for contactless payment the charge is made from the debit side.

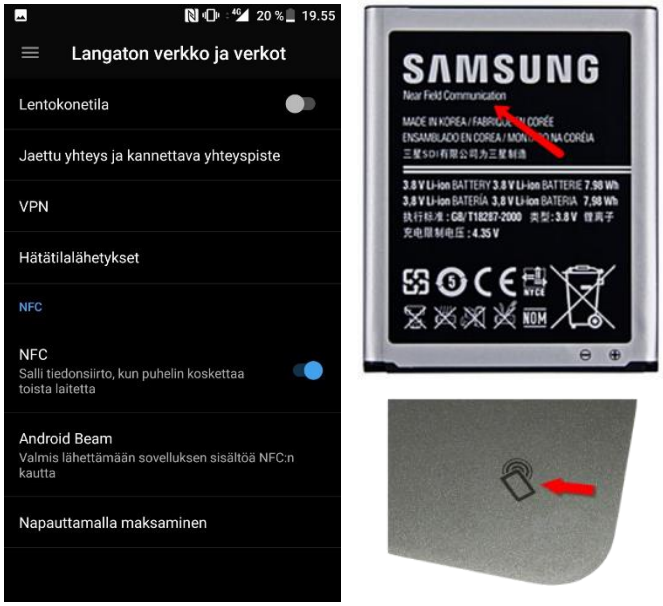
(Figures 4-7. In order: debit, credit, electron and the combination cards by Nordea. Nordea 2017)

2.2 Mobile phones

The earliest forms of mobile payments worked in a way where the sum of the purchase was added to the subscription owners mobile bill. With development of NFC add on devices, NFC stickers and built-in NFC tags the forms of mobile paying have increased. In addition, with the latter forms of mobile payment some applications offer payment options as well, such as mobile pay, ABC-mobiilitankkaus etc. Since we are considering the forms of contactless payment and in particular NFC payments I'm going to through some key factors in NFC payments with mobile devices and methods.

2.2.1 Mobile phone devices

Today there's a lot more mobile phone brands than there were in the golden 90's and early 2000's so I'm not going to list them all in here. Basically, a good ground rule is that most if not all android phones have a NFC antenna built inside. For example, Apple phones, do not support NFC, for they have developed their own EMV Payment Tokenisation Specification. (Apple 2017). Most mobile phones have a logo or the text Near Field Communication on the battery to tell about the availability and the user can also find out about it in the phone menu as such: (Weebly 2017)



(Figures: 8-9 The menu of an android phone (Oneplus 3T) and a Samsung Battery. Own screenshot & Weebly 2016)

In order to turn the NFC option on, the user only needs to enable it from the phones menu. In addition to the android phones, also Nokia's Microsoft and Lumia phones also had the NFC antenna built inside. To be more technical, in the android NFC stack there are two implementations of a built-in NFC chip available. The models are "libnfc-nxp" and "libnfc-nci" (J. Vila & R.J. Rodriguez 2015).

2.2.2 Tablets and Laptops

Some laptops and tablet devices also have a NFC antenna built inside, but in those cases the format is to read for example a card or another NFC device and they aren't used as the actual paying or checking in device. Most laptops and tablets that have NFC technology utilize the technology for reading other NFC utilizing devices like id cards for identification, travel cards for topping up the value like the Oyster card or HSL card. It's also common that NFC is used for data transfer, but for that purpose it's really slow and can be awkward. (Weebly 2017).

3 The Technology

3.1 NFC Technology

Near Field Communication is a similar type of wireless communication form as Bluetooth and Wi-Fi. The exception is that the range is a lot smaller and the form of communication is done by sending and receiving radio waves. NFC originated from the RFID technology invented in 1983 by Charles Walton (Google patent registry 2017) which in a way it also utilizes today. RFID stands for Radio Frequency Identifier. Basically "NFC is similar technology, but standardized for consumer smartphones" (Matt Egan 12.5.2015). What Matt is referring to is that RFID technology is widely used in warehouses and stores where the worker can scan the contents of a cargo box utilizing RFID in other words, in industries.

NFC works with electromagnetic induction by making a connection between two devices via radio frequency running at 13.56 megahertz. The radius of the devices can be a maximum of 3-4cm and the connection, unlike for the RFID which only reads information the NFC has also a read and write connection. So, the communication can go both ways. The connection speed when it comes to data transfer is 106.2kb/s, 212kb/s or 424kb/s which in internet broadband speeds is relatively slow but in data communication sufficient. The speed is approximately the same as the standard GRPS (30-114kb/s) or EDGE (80 – 236.8kb/s) network speeds. In the NFC data transfer protocol, there always must be two devices and two modes active: the initiator and the target, where the initiator is the active party during the whole data transfer process and the target remains passive. Since NFC can send electric currents the passive party does not need to have any energy or a power source whatsoever.

3.1.1 NFC Modes

NFC devices that are fully compatible can operate in three different modes:

- Read/Write mode:

  The mode is used for embedded NFC tags like in posters or labels. The functionality is pretty similar to QR-codes, but utilizing the NFC technology. In this mode, the reading NFC device reads stored data from the tag.

- Peer-to-Peer:

  Is used for when two devices communicate with each other and transfer data. A good example of this is when a person who buys a new android phone wants to transfer all the information from the old phone to the new phone he can activate the NFC on from both “peers” and perform the data transfer

- Card Emulation

  Card emulation enables the NFC device to act as a card, such as a bank card or a travelling card etc. When it comes to NFC payments with devices other than actual bank cards, this is the most common mode. (Cameron Faulkner 2015)

In total, there are also two main NFC elements which are: Proximity Coupling Device or PCD this can be an any NFC enabled device such as a smart phone. And Proximity Integrated Circuit Cards or PICC which is usually a NFC tag or a sticker You will find out more about the tags and stickers later from the “beer festival” example.

3.1.2 NFC Protocols and the Protocol Stack

The NFC protocols can be described as a complex set. Even though for the end user NFC as a technology is great, for the developer it can be a nightmare. Historically there’s been multiple different developers generating their own specifications and compatibilities during the last twenty odd years, which for today has resulted in incompatibilities and multiplicity of pre-existing tags and features.

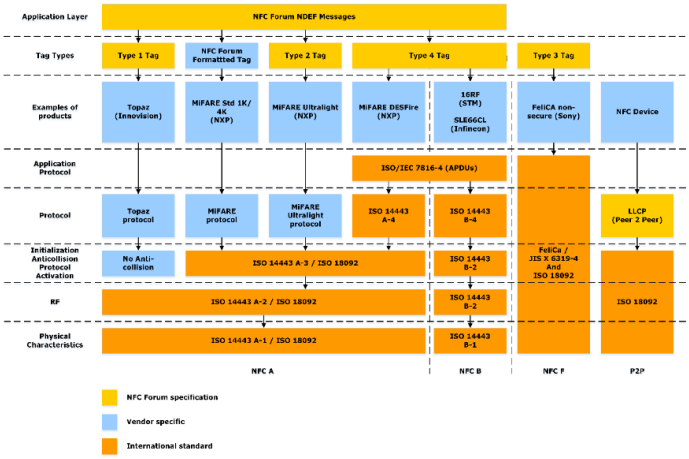
The communication protocols and data exchange format standards in NFC are based on the RFID standards. The Standards are loosely defined by the non-profit organization NFC Forum which was formed by Philips, Nokia and Sony in 2004. The protocols used in NFC protocol stack are: Topaz protocol, MiFARE and MiFARE ultralight protocols, LLCP

protocol and the ISO 14443 A-4 and B-4 anti-collision protocols. As for the standards, the NFC uses ISO 14443 A-2 / ISO 18092 and ISO 14443 A-1 / ISO 18092 standards. The exception in the stack as mentioned earlier on manufacturer specific uniqueness's is the Sony's FeliCa protocol model, FeliCa is a RFID smart card reader system. These standards specify the whole of NFC process and details from modulation schemes, transfer speeds, frame formats, coding and the conditions for data collision control.

The protocols vary depending on the platforms and the NFC mode in use, which also defines what NFC tags are used. In total, there are 5 different types of tags which are used for different vendor's products and vendor specific protocols. Each type of tag has its own capabilities and restrictions that affect the use of memory, messaging and maximum size etc. In addition to the pre-existing standards there has been new protocols and formats developed.

For example, the most simplistic NFC mode the card modulation should send and receive information, in this case at least a unique flag or an id. For this purpose, the NFC Forum has developed a data format called NDEF or NFC Data Exchange Format. The NDEF can store and transport any ASCII, MIME (any other data then text for example), URL's and such. And for the card emulation mode the NFC developed a NDEF Exchange Protocol or SNEP to specifically allow the receiving and sending of messages between two different NFC devices. As in modern day business the NDEF and SNEP were developed to simplify the transfer protocols.

Basically, the NFC protocol stack is so confusing because there are so many different types of pre-existing protocols that have been implied and almost none of them work with each other. For example, android doesn't support LLCP level via API but it supports SNEP API etc.



(Figure 10: The NFC Protocol Stack Wikipedia 2017)

3.1.3 Tag and Product Explanations

- **Type 1 Topaz** – Type 1 tags use a topaz protocol. There are two memory models for it to use, either a static memory mode for tags that have memory size less than 120 bytes or dynamic mode for tags that have larger memory. Bytes are written by simple commands like WRITE-NE, WRITE-E8, READ, RALL etc.

- **MiFARE Classic** – MiFARE classic or old tags are basically for storage devices. The original security controls were broken in 2007 which resulted to MiFARE classic not being used that much anymore.

- **Type 2 MiFARE Ultralight** – Action wise similar to type 1 tags with the exception that when the tag has less than 64 bytes available it uses static mode and otherwise the dynamic mode. The first 16 bytes of memory is always meant for metadata such as access rights etc. READ and WRITE actions are used to access data.

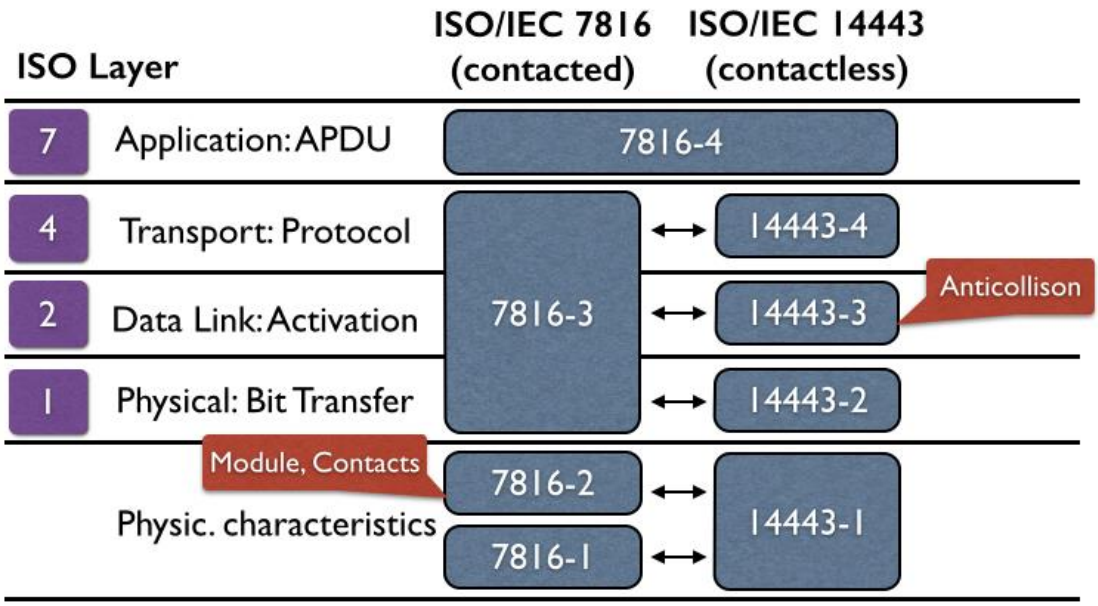
- **Type 3** – Type 3 tags are very rare; the only known exception was the manufacturer built Sony FeliCa which is mainly used for access points such as work places etc.

- **Type 4 DESFire** – Type 4 tags always contain at least two files, the CC or the capability container and the NDEF or NFC Data Exchange Format file. The tag is designed to fill the purpose of reading the CC file which then tells it what to do with NDEF file. Commands are SQL influenced like “Select, ReadBinary, UpdateBinary”.

- **LLCP Peer 2 Peer** – Logical Link Control Protocol works in a very different and more intelligent way than the previously mentioned modes and tags. In the previous versions, there has always basically just been a read / write operation, when the LLCP protocol is for connecting two communicating devices and maintaining the connection even if there are no packages being sent or received. It can perform a connectionless or a connection orientated connection using commands such as CONNECT. There are also some variations to different kinds of LLCP’s.

3.1.4 Example: ISO 14443 standard

The ISO/IEC 14443 standard is used mainly for the most common NFC Payment type: Contactless payment cards. The standard is a 4-part international standard for all contactless smartcards. The four parts define such factors like: data transmission protocols, RF power and signalling schemes, Initialization and the anti-collision protocols and the size and characteristics of the packages.



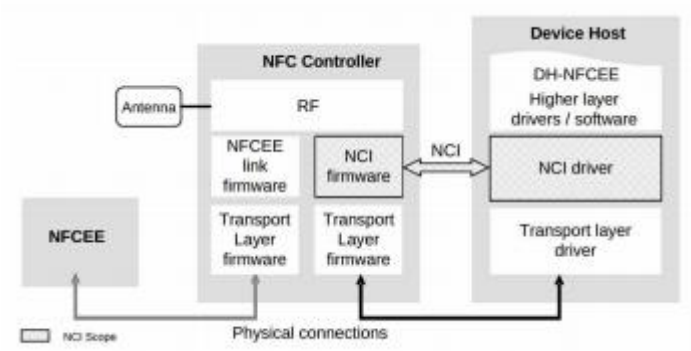
(Figure 11 the ISO/IEC 14443 stack. Protocolbench 2017)

3.1.5 Android NFC stack

At this point of the thesis it is important to look in to the android NFC architecture and stack, for this information is very useful later when describing attack scenarios and methods. As mentioned earlier the NFC chip built inside the android device determines the native implementation that is in use. These two native implementations are:

- **libnfc-nxp (NXP**) - NXP is an implementation that provides support only for NXP PN54x controllers in the NFC architecture as well as NXP MiFARE products, but due their rarity and the specific transmission protocol it is not that widely used.
- **libnfc-nci (NCI)** – NCI provides support for any NFC Controller Interface compliant chips. NCI is also more widely used today because it has very little limitations concerning chip families and it provides an open interface between the NFC Controller and device host.

The NCI is widely supported as the standard by the NFC Forum, the non-profit organization mentioned earlier. This widely because NCI specifications aim to cut down the compatibility problems and make the NFC chip integrate with as many as possible manufacturers devices with a standardised level of performance. In a way, you could call it the “open source” of NFC development. “It also provides a logical interface that can be used over different physical channels, such as UART, SPI, and I2C.” (J. Vila & J. Rodriguez 2015). Other notable facts about what lead to the NFC forums favoring of the NCI are for example Google deciding to use it in its latest models of Nexus phones and the overall performance between NFCEE’s (NFC Execution Environment) and connectivity through RF channels. The NCI NFC developer framework also allows the use of C++, C and Java across platforms so the diversity has lots of advantages over NXP.



(Figure 12 the NCI communication form. J. Vila & J. Rodriguez 2015)

NFC Technology is constantly being developed into more complex and more secure it wise, but the foundations are in the RFID technology developed in the 80’s. On hardware level the development is slow paced comparing to the software level. It is though in the software level that the security issues can more effectively be tackled. The sole NFC pieces of technology have very little safety aspects or features built in and the performance depends entirely on the mode a PCD or PICC is set at. It is the constant battle between the exploiters and those who work to enhance security on the software level that define the safety of NFC and especially NFC Payment Methods. In the following chapters the thesis will go through known security issues, known cases, experiments (of my own and ones that are already done) and conduct a research of the public knowledge about NFC security measured through an open survey.

4 NFC Security Threats & Methods

In this chapter I will go through the most common un-imaginary NFC security threats, which have example cases and have been done. I will also play around with some theories that security specialists have come up with. As it always is in IT-security the crooks are one step ahead of the security authorities, so in that sense of thinking it's not at all farfetched to consider the threats that have not yet been conducted, but which may be possible to conduct in the future.

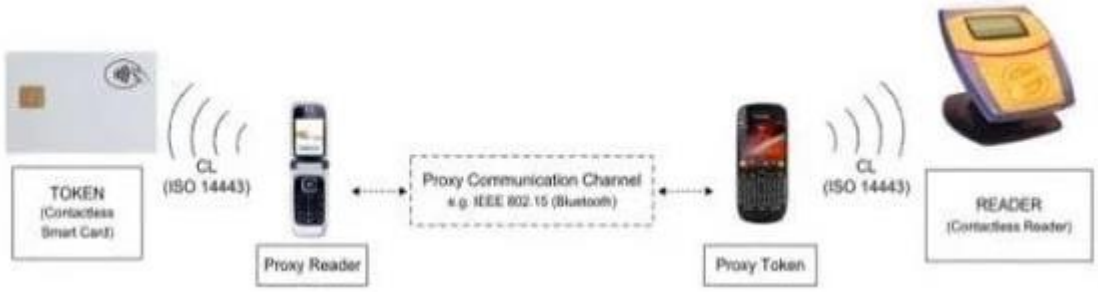
4.1 Debit/Credit Card Data Theft

Probably one of the most feared actual forms of attack which enables the largest profit for the attacker and the largest loss for the victim. This form of crime was very visible in the headlines in February 2017 with front page news stories by: "Ilta-Sanomat, Iltalehti and Helsingin Sanomat". (IS 2017). The technology and method for credit card theft is rather simple because of the security gaps in the NFC safety.

This form of security threat can lead to loss of credit, data corruption, spoofing and man-in-the-middle attacks as said by cyber security expert Pierluigi Paganini (Security affairs 2015). For the attack to be successful the attacker would need two devices: an android phone with NFC and a card reader that can charge money like the ones talked about earlier in the "NFC devices chapter" and a victim.

4.1.1 The Attack Scenario

As tested by Pierluigi Paganini in 2015 the attacker needs the two devices talked about earlier which in more detail are: PoS device with GRPS and NFC Support and should make sure that the android device is running Android 4.4 KitKat interface or a newer version. First the attacker launches a relay attack, which is a form of hacking related to the man-in-the-middle. The relay attacks purpose is to manipulate the communications between two parties in this case the victims phone and credit card. Pierluigi describes that the concept in use is the "the honest prover, the honest verifier, the dishonest prover, the dishonest verifier" (Security Affairs 2015). In this case the dishonest communicators are used to trick the honest ones. To assign the roles to actual items: The mobile of the victim is the dishonest verifier, the attackers mobile is the dishonest prover, the portable payment reader is the honest verifier and the victims credit card is the honest prover. Now at this phase it's good to be clear that this sort of attack requires very specific circumstances to "work" but I will go through the technical details after the timeline description of the attack.



(Figure 13 the devices and roles Security Affairs 2015)

Once the victim is selected after the environment scan and the successful relay attack, the next step is to make the victim download an app specifically designed to scan the near (NFC) area around the infected mobile phone. There's two ways to make the victim download the app, one of which per google (IS 2017) has been patched. One way is to infect the victims mobile with a Trojan virus that will force download the app to the mobile, or use similar techniques that are used in the phishing form of hacking. In this case persuade or trick the user to accept the apps download manually. All of this done through the previously formed connection.

```
V → P 00A4 0400 0E32 5041 592E 5359 532E 4444 4630 3100
P → V 6F2D 840E 3250 4159 2E53 5953 2E44 4446 3031 A51B BF0C 1861 164F 07A0
      0000 0003 1010 500B 5649 5341 2042 414E 4B49 4190 00
V → P 00A4 0400 07A0 0000 0003 1010 00
P → V 6F33 8407 A000 0000 0310 10A5 2850 0B56 4953 4120 4241 4E4B 4941 9F38
      189F 6604 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 0490 00
(messages omitted for privacy issues)
V → P 80AE 8000 2B00 0000 0000 0100 0000 0000 0007 2480 0000 8000 0978 1502
      2400 37FB 88BD 2200 0000 0000 0000 0000 001F 0302 00
P → V 7729 9F27 01XX 9F36 02XX XX9F 2608 XXXX XXXX XXXX XXXX 9F10 12XX XXXX
      XXXX XXXX XXXX XXXX XXXX XXXX XXXX XX90 00
```

(Figure 14 the timeline of the relay attack used for copying a MasterCard using two android devices and a PoS-machine. V = verifier, P = Prover. Hitb-Conference 2015)

Once the app is downloaded the app starts to scan the surrounding areas. In this phase for the attack to be successful the victim's mobile needs to be close to the victim's wallet that has the credit card inside of it. If the app recognises that there is a credit card in the close proximity of the mobile it uses the previously formed connection to send a notification to the attacker's smart phone. At this phase since the app has copied the credit card credentials the attackers mobile phone acts as a credit card replica and the now the attacker can just use it for the PoS machine and start making numerous 25€ - 100€ transactions depending on the card of the victim. In Finland, the sum would be >25€.

4.1.2 Analysis & Protection

At the moment, it would seem that NFC technology for payments is being pushed to the markets faster than the security requirements are met. Such is the case with relay attacks as well. As researchers Jose Vila and Ricardo J. Rodriguez stated in their research *"Unlike eavesdropping or data modification, relay attacks are a threat that may bypass security countermeasures, such as identification of communication parties or cryptography schemes."* (Hitb-Conference 2015). To put some facts on the table, "nfcworld.com" predicted that in 2019 there will be over 500 million NFC users worldwide and almost 300 different mobile phone models available that use NFC technology. The explosive growth in the technology available has also created such security risks as this scenario. Even though the current NFC payment rules only allow 25€ to 100€ transactions, the attacker has time to conduct numerous charges before the PIN code is required. And that alone makes it a serious risks, at least when the attacks are being made on a large scale.

4.2 Eavesdropping

Eavesdropping is a method of an attack that does not necessarily focus on stealing information or personal or financial damage for the victim. An eavesdropping attack can be used to disrupt and block communications between two NFC devices or to corrupt the data that is meant to be transferred between the devices. In that sense an eavesdropping attack can also very much remind of a DoS-attack (denial of service) where the main goal of the attacker is to make the wanted transaction or communication unavailable. For the attack to be successful the attacker must be able to break the secure channel between the two devices using encryption methods and the device used for the attack must be in somewhat close proximity. This kind of attack could well bring chaos to event holders if NFC is the main method to buy the tickets or the tickets themselves only use NFC technology. The risk for the attacker is that the proximity factor makes it riskier and the attacker can be potentially easily recognized.

(Figure 15 Eavesdropping attack scenario INFOSEC Institute P. Pagani 2015).

4.3 Data Modification & Data Corruption

Data modification is very similar to eavesdropping and eavesdropping is basically the same as data corruption. In a data modification attack the difference is that the data that is being exchanged between two devices is to be modified in order to benefit the attacker. The way it works is that the attacker can use a RFID jammer to briefly exchange data and to alter the binary coding of the original exchange. Researcher P. Pagani describes “This type of attack is very difficult to implement but the data modification is realizable in rare cases” (P. Pagani 2015). He tells in his study that the way to notice an attack of this sort is to introduce a code to the NFC device that measures the strength of the frequencies “thus choosing the one that is truly the closest and most likely valid”. (P. Pagani 2015). Even though a data modification attack is incredibly hard to notice for a regular end user it also extremely hard to conduct. There are many factors that need meet as stated by researchers Ernst Haselsteiner and Klemens Breitfuß in their paper “Security in Near Field Communication (NFC) – Strengths and Weaknesses” (2013).:

- The strength of the amplitude modulation
- Transferring data with Miller coding, only certain bits can be modified.
- Transferring Manchester-encoded data with a modulation ratio of 10% permits the modification of all bits.

Unlike in your standard MITM credit card theft attack scenario, for data modification the attacker needs to be very skilled in many aspects to conduct a successful attack.

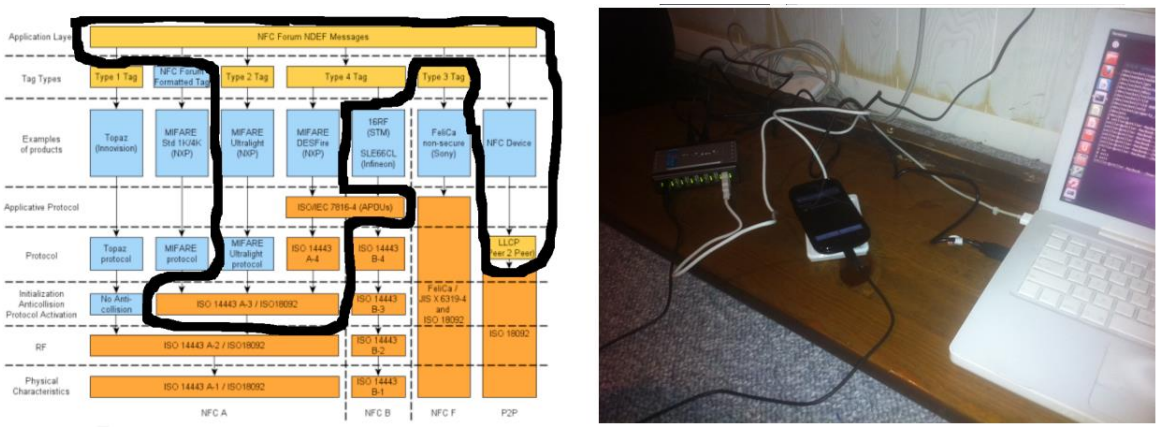
4.4 NFC Protocol Stack Fuzzing & Android NFC Stack Bug

The NFC stack fuzzing attack is done by the attacker's interception of the communication between the victim's device and the NFC protocol stack. The attack is very unlikely to be successful but in theory if succeeded the attacker could exploit ordinary NFC operations such as purchases at the cashier or agency. The attacker needs either to be in close proximity or an antenna to do a NFC protocol stack fuzzing attack. There are also other exploits to fuzzing attacks that could end in the attacker having total control of the victim's phone through NFC. As Pierluigi Pagani states when describing fuzzing, the attackers NFC device: "… analyses the software that is built on top of the NFC stack for victims' devices." He then continues to describe the full effect an attack can have:" An attacker can force some mobile devices to parse images, videos, contacts, office documents, and even any other content without user interaction." Other actions that the attacker can do include making phone calls and texting, which also is a major security risk given that the attacker might have a pay-per-call number that charges the victim drastic sums when dialled.

Android NFC Stack bug works in a rather similar way but with few exceptions. An American hacker Charlie Miller published a proof of concept "Exploring the NFC attack surface" in 2012 where he made several attacks to various android phones in various ways. One described method the NFC stack bug works in a way where the attacker exploits the flaws in the phones Bluetooth pairing settings and the victim scanning a NFC tag that the attacker has planted.
In this case Charlie used a Nokia N9 mobile phone with NFC enabled to connect to the phone. The attacker sends a NDEF message to the victim's phone, in it's all simplicity something like the following:

[0000] d4 0c 27 6e 6f 6b 69 61 2e 63 6f 6d 3a 62 74 01 ..'nokia.com:bt.
[0010] 00 1d 4f 92 90 e2 20 04 18 31 32 33 34 00 00 00 ..O… ..1234…
[0020] 00 00 00 00 00 00 00 00 00 0c 54 65 73 74 20 6d …….Test m
[0030] 61 63 62 6f 6f 6b acbook (Charlie Miller 2012).

Charlie describes the test message as following: ""In this message, a PIN is given as "1234", a Bluetooth address, and a name of the device are also provided. Once paired, it is possible to use tools such as obexfs, gsmsendsms, or xgnokii to perform actions with the device." (Charlie Miller 2012). And what it means translated is that the attacker has the total control of the victim's phone without the victim even knowing about it.



(Figure 16 The fuzzing scenario and fuzzing attack setup Charlie Miller 2012).

In the figure 16 on the right we can see the layers of the NFC protocol stack where the NFC fuzzing attack concentrates in and on the left, we can see how simple hardware wise a setup for a fuzzing attack can be. The setup is the one Charlie Miller used in his experiments in 2012.

5 Study One – The Survey

I conducted a research in the form of a survey about how do ordinary consumers use NFC payment methods and how safe do they think that NFC payment methods are. The research was orchestrated in a quantitative method, and before the survey started I set a limit of at least 50 answers needed to the survey to get a proper result. In research terms a survey is “a brief interview or a discussion with individuals about a specific topic”. (Study.com 2017). The goal of this and any survey is to collect a passible amount of information concerning the chosen topic. The survey itself was done so it would be fast to do and to get specific answers, the simplicity of the survey was so that as many as possible people would complete it. From my previous experiences, I determined that on average people lose interest quickly and a long dragging survey would cost me some answers.

The survey was done via internet survey platform called “surveymonkey.com” and all the analysis was done on excel and other analysis tools. The latter was because of the surveymonkey.com websites free and premium subscription options of which the latter would’ve demand a 20€ fee, so I went with the free one. The platform is in Finnish as well as the questions I conducted to the survey, I felt it was necessary for most of my friends aren’t that familiar with NFC or especially NFC in English. The survey consists of six questions, each question having multiple choice answers, some questions with multiple options and some having a free form text field where the surveyors could type in something relevant that wasn’t on the pre-determined answers.

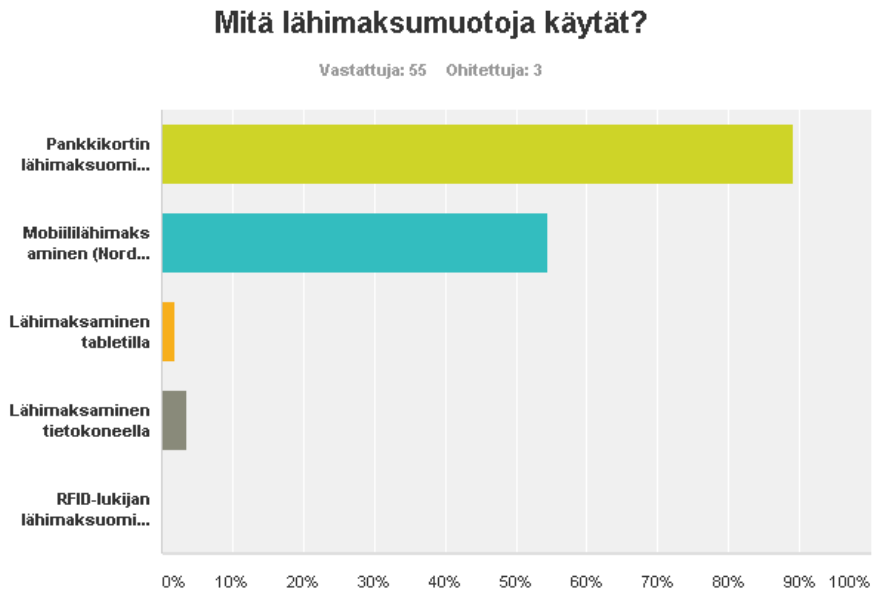
The survey was online between the 9th of March and the survey was locked on the 15th of March. During the time period the survey got 58 answers. The survey could be found from a link which I shared on various social media platforms including WhatsApp, Facebook and Twitter. The survey itself was IP coded, so that one person could only submit one set of answers through one IP address. The geological distribution of the people who answered the questions located between Oulu and Helsinki. Because of the language barrier there were no answerers from outside Finland. This chapter will be divided in to seven parts; each question has its own section and the conclusion has the final section. I also gathered graphs and data from the survey which I will present on this chapter as well. Figures are entirely in Finnish so translations are found from the text.

5.1 Question one – Which forms of close contact payment have you used?

The first question was conducted to map all the different payment methods the people use. The options were: debit/credit cards, mobile phone and apps, tablet device, NFC on a computer and using a RFID reader.

5.1.1 Analysis of the results

The answers were expected and the distribution between the answers very low. 89.09% of the people who answered the question chose debit/credit card, which seems to be the most used form. What surprised me a little bit was the popularity of different mobile phone apps and NFC payments. In total 54.55% of the people who answered use mobile paying methods as well. On the bottom of the barrel was RFID readers which probably due to its incredibly hard to buy nature no one chose as the answer. This question also had a free form field where one could specify if any other form of close contact payment is in use. Only one free form answer was submitted, roughly translated “I would use it on my debit card but my bank does not offer the option”.



Vastausvaihtoehdot	Vastaukset	
Pankkikortin lähimaksuominaisuus	89,09%	49
Mobiililähimaksaminen (Nordea Pay, Pivo, MobilePay etc.)	54,55%	30
Lähimaksaminen tabletilla	1,82%	1
Lähimaksaminen tietokoneella	3,64%	2
RFID-lukijan lähimaksuominaisuus	0,00%	0
Vastaajat yhteensä: 55		

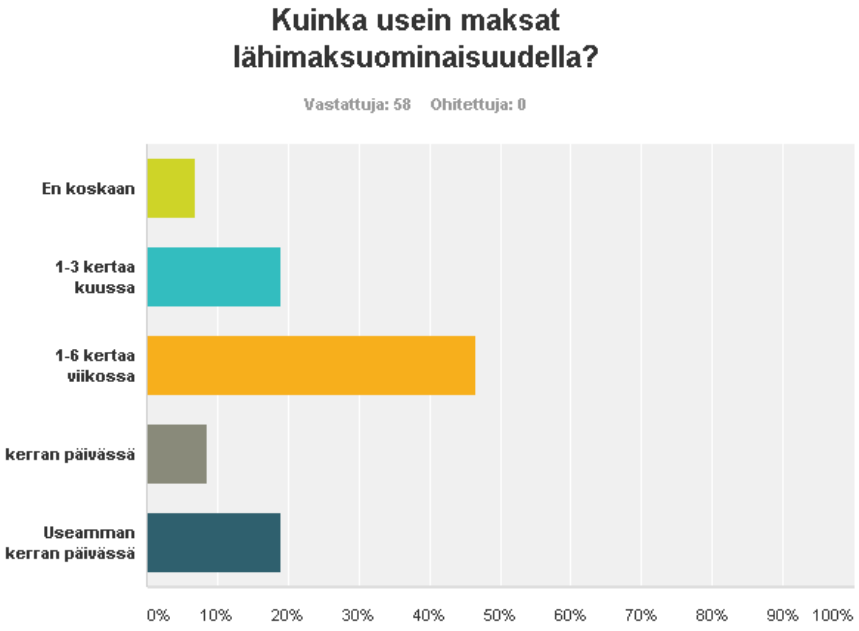
(Figure 17 Question 1)

5.2 Question Two - How often do you use contactless payment?

The second question was conducted to map the frequency of the using of contactless payment methods amongst the answerers. The options given: Never, 1-3 times a month, 1-6 times a week, once a day or more than one time per day. The answerers were also guided to use their best judgement on the answers and estimate the average of their use. In this question the person answering could only choose one option.

5.2.1 Analysis of the results

There was a decent distribution amongst the answers, the most common options chosen was 1-6 times a week with a share of 46,55% people choosing the option. One noticeable factor was that 4 people chose the option never which made some questions irrelevant for them. There was an exact equal share of people who chose the option 1-3 times a month and those who chose more than one time a day.



Vastausvaihtoehdot	Vastaukset	
En koskaan	6,90%	4
1-3 kertaa kuussa	18,97%	11
1-6 kertaa viikossa	46,55%	27
kerran päivässä	8,62%	5
Useamman kerran päivässä	18,97%	11
Yhteensä		58

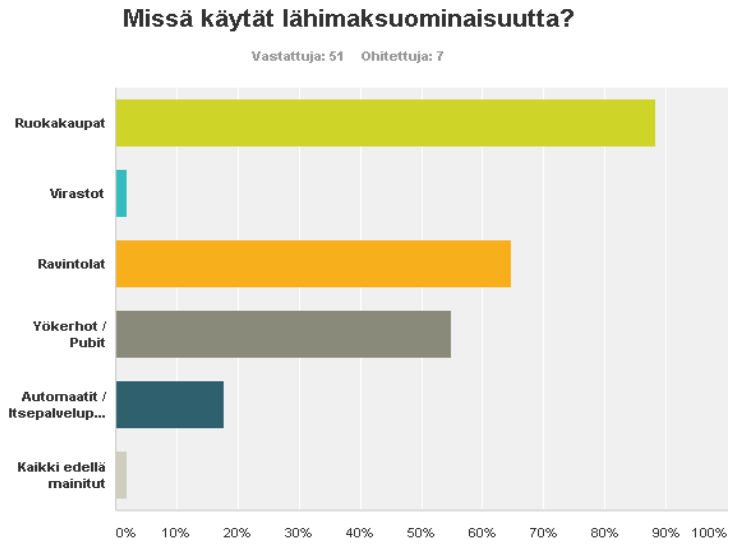
(Figure 18 Question 2)

5.3 Question Three – Where do you use contactless payment?

This question was conducted to start mapping the security matters. I think it's relevant where do people use NFC payment methods for it correlates to what people think are the safe places to use it. In this question the options are: Grocery stores, Agencies, Restaurants, Pubs and nightclubs, self-service automates and vending machines or all the above. On my behalf, it must be said that the all the above option could've been left out since it distorts the results but luckily only one answerer chose that option. In this question the answerer could choose multiple answers. There was also an option to write on a free form field as "other" option.

5.3.1 Analysis of the results

A whopping 88.24% of the people who answered chose grocery stores as the payment location of choice, closely followed with restaurants 64.71% and pubs and nightclubs with 54.90%. Agencies were the least chosen option and I can say from my own experience that that might be due to the lack of the option when considering agencies like the police station, public transport agency etc. On the free form fields, there were 10 answers and the answers varied between: "Workplace cafeteria" which would have fallen under the restaurants category and transfers between friends which can be done using NFC and an appropriate app.



Vastausvaihtoehdot	Vastaukset	
Ruokakaupat	88,24%	45
Virastot	1,96%	1
Ravintolat	64,71%	33
Yökerhot / Pubit	54,90%	28
Automaatit / Itsepalvelupisteet	17,65%	9
Kaikki edellä mainitut	1,96%	1
Vastaajat yhteensä: 51		

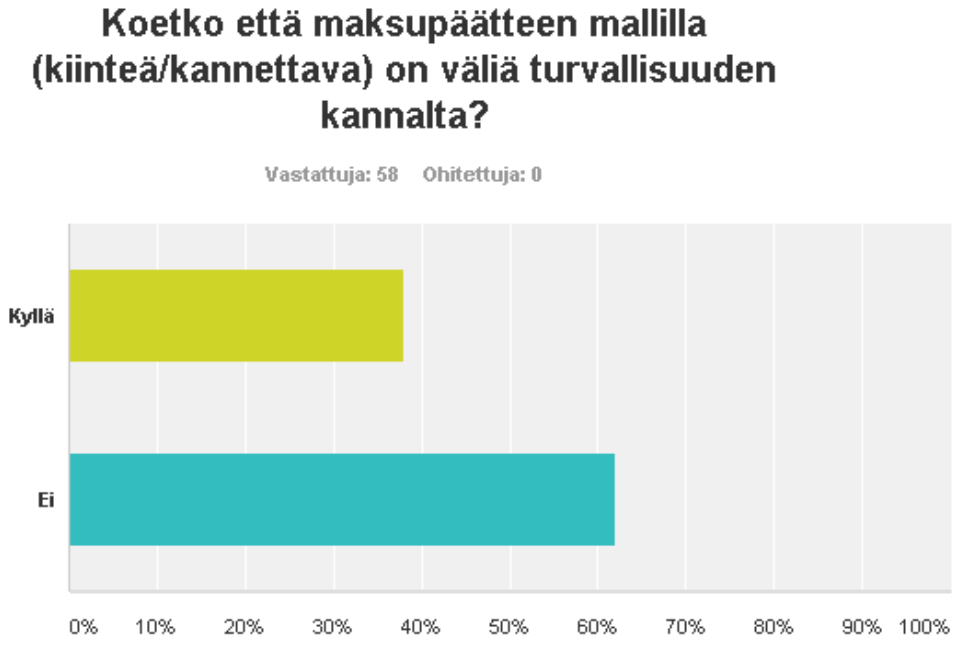
(Figure 19 Question Three)

5.4 Question Four – Does the model of the reader make a difference security-vice?

This question was conducted to gather information about how do people feel about the different payment readers and their security aspects. For example, a solid mounted reader that you would find from a grocery store, might to some feel a lot more secure than a mobile reader that you would use when paying the pizza delivery clerk or an outdoor bartender. There were only two options on this question and only one option could be chosen.

5.4.1 Analysis of the results

The results were almost fifty-fifty but not quite. 37.93% of the people answered felt like there is a difference in the security between a mobile and mounted NFC readers and 62.07% felt like there was no difference. When I was considering whether to add this question or not, I had come up with it just because of my own superstitions but the results show that I was not the only one who considered the possibility that there is a difference.



Vastausvaihtoehdot	Vastaukset	
Kyllä	**37,93%**	22
Ei	**62,07%**	36
Yhteensä		58

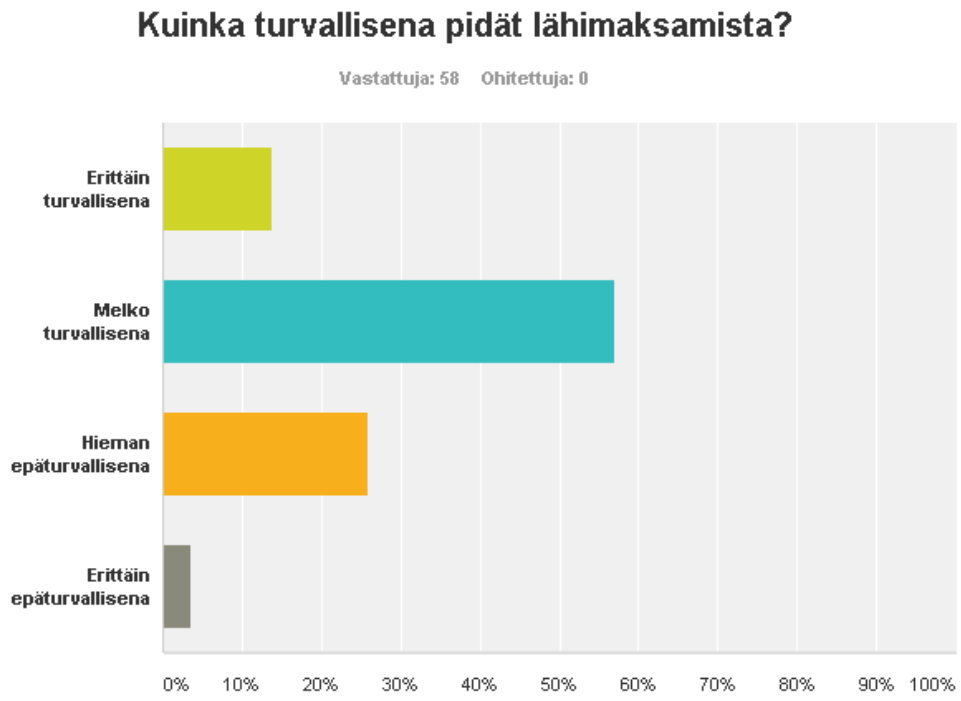
(Figure 20 Question Four)

5.5 Question Five – How secure is contactless payment in your opinion?

The fifth question was conducted to get an overall view of people's opinion about the security of NFC payment methods. In this question, there were four options: Very secure, somewhat secure, somewhat unsecure, very unsecure. The options were made vague to represent the percentage limits as quarters. In this question the person could answers only option.

5.5.1 Analysis of the results

The majority of people think that NFC payments are somewhat secure. The result was expected for the knowledge of an average person on NFC security issues is not that broad. Overall 56.90% of people chose somewhat secure as their answer. Quite surprisingly 3.45% chose very unsecure as their option and it could be explained to be due of all the headlines about security issues on credit cards that have been published lately.



Vastausvaihtoehdot	Vastaukset	
Erittäin turvallisena	13,79%	8
Melko turvallisena	56,90%	33
Hieman epäturvallisena	25,86%	15
Erittäin epäturvallisena	3,45%	2
Yhteensä		58

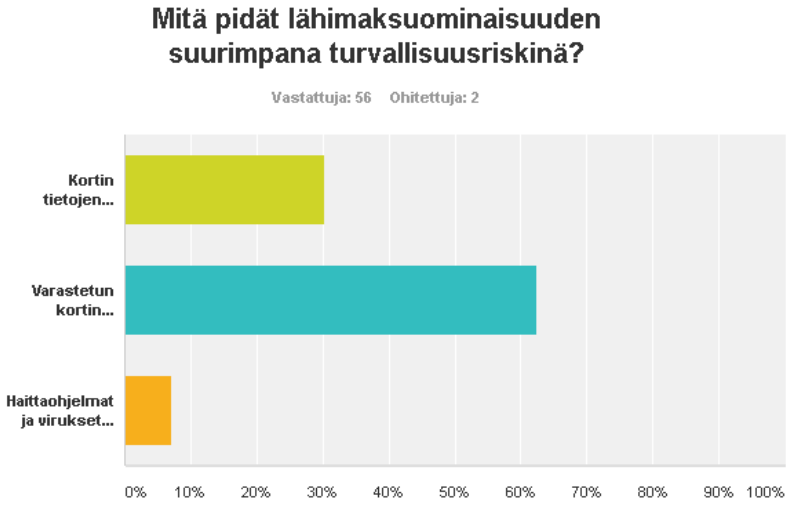
(Figure 21 Question Five)

5.6 Question Six – The biggest security risk in contactless payment?

The question was conducted partially to test whether people know the different possibilities they can fall victim to fraud and to map the answerers consideration of the biggest security risks involving NFC. This question had three options to be chosen from, the person could choose only answer and the question involved a free form text field for other answers. The three options were: Copying of the card information, Misuse of a stolen card and viruses and malware.

5.6.1 Analysis of the results

The most common answer was somewhat natural, 62.50% of the answerers chose the misuse of a stolen card as the biggest risk in NFC. And to be fair it is a big, but somewhat manageable risk. A person can use the NFC ability of a debit/credit card only for purchases under 25€ and only 3 times within a short period before the reader requests a pin code. (Nordea 2017). Second biggest risk was identity theft or copying of card credentials which then could be used online for making larger purchases. 30.36% of people chose the latter option. From the free form fields one answerer said “All the above” which then again is pointless, because the question was about mapping the single biggest threat or risk. There are some other risks as well, but most relatively uncommon so I left the options out of this question.



Vastausvaihtoehdot	Vastaukset	
Kortin tietojen kopiointi (esim. lukijalla lähietäisyydeltä)	30,36%	17
Varastetun kortin väärinkäyttö (useat n.25€ ostokset)	62,50%	35
Haittaohjelmat ja virukset (koskee laitteita)	7,14%	4
Yhteensä		56

(Figure 22 Question Six)

5.7 Conclusion

So, to draw some conclusion about the survey we need to analyse the group and marginalise the people in different categories. I will make divisions judging by the geographical aspects, age groups and then make an analysis out of those factors. The people who answered the survey were all from Finland, 3 people from Oulu, 25 from Järvenpää and the rest from Helsinki. The age distribution varied from the youngest answerer who was 19-years old to the oldest who was 53-years old, the average age rounded was 29-years old. Out of the 58 people who answered the survey about half were students and the other half in working life. Overall the distribution could've been broader but in the timeframe given there was enough variance.

The analysis of use frequency and method types show that most people out of my target group use debit/credit cards as the main device for NFC payments, the most common place to use an NFC device to pay is the grocery store and most use NFC payments almost daily.

To analyse how the average people who use NFC payment methods feel about the security aspect of NFC I analyse the results through some follow up questions to some randomly picked answerers. From the further discussions, I got the impression that media and news outlets are responsible as the main reason for the security threat fear, not any scientific or proven factors. This lead to the need to analyse the mainstream media newsfeed concerning NFC topics during the last 6-12 months and analyse which news might've affected people's thinking the most and then go through from a scientific point of view what the news suggests. Is the news so called "fake news" or accurate?

5.8 The news, examples of NFC stories

Upon further investigation, I noticed there had been several news stories about the security threats of NFC payment during the last years so I will go through two cases and a few more headlines. There are multiple other news stories from outside Finland but since the scope would be too wide I will only concentrate on the Finnish news stories.

5.8.1 Case: After Pay Bracelets

In the summer of 2016 at the beginning of August there was held an event at Rautatientori in Helsinki called “small breweries, large beers”. The event launched a brand new paying method to be used throughout the festival that utilises NFC technology. The organizers distributed a “AfterPay Bracelet” to all the festival goers which included a NFC tag, meant to keep record of the “tab” of the visitors. So, to put it simply the festival goers could drink as many beers as they wanted and record everything with the AfterPay bracelet which was activated for each person using personal information details like social security number, home address etc. And then after the festival the invoice would be sent to the festival goers home address.

The bracelets featured NXP MI FARE Classic 1k NFC tag and protocols but the design lacked some crucial features that you would normally find from a NFC abled debit card. The bracelets did not have any safety measures for copying, there was no double secure measures like pin code required and there was no limit set for the maximum sum that the bracelet could pay, so the bracelet owner could make purchases over 25e.

The misuses were done by using cheap 1€ NFC tags that anyone can buy from China for example and a normal android phone that has an NFC tag built in. The way that some misuse was carried out was that the copier/misuser could copy the information from another person’s bracelet using an NFC application on the android phone and selecting the copy option. After the copy process was done, which would take approximately few seconds the information from the victim’s bracelet were than pasted on to the Chinese NFC tags, which then could be hidden and glued under the misuser’s bracelets, only then the misuser wouldn’t have been using his own tab, but charging the victims tab all the time. The victim would’ve only find out about the misuse after the event when receiving the invoice. The security risk was first reported by Harry Sintonen on his blog (Sintonen 2016) and later brought to larger audiences by Ilta-Sanomat’s format Talous sanomat (IS 2016).

(Figure 23 an AfterPay bracelet)

5.8.2 Case – Crowded trains and successful payment with a closed card

On the 30th of April in 2016 Oululehti published a story where a man from Oulu had tried and succeeded in charging his debit card after the debit card had been terminated. (Oululehti 2016). In the story the man from Oulu is left unnamed so we'll call him Seppo. Seppo had a standard visa debit/credit card in use, which he had terminated. Disregarding of the termination Seppo tried to see if the cards contactless payment still works and it did. The card had originally been terminated by Seppo himself because of fear about a scimming attack on his card at a local gas station.
Because of the incident Seppo contacted Oululehti, a regional news outlet in Oulu and which then contacted a "team leader" in OP, Osuuspankki. Pekka Nummela from Osuuspankki described that what had happened is not out of the ordinary, but then continued to state that "Contactless payment on the debit side is very restricted". (Pekka Nummela Oululehti 2016). By which he meant that the security measures of contactless payment do not allow purchases over 25 euros without the pin code of the card. Even though the limit is set at 25 euros the scammer can still perform multiple under 25 euro purchases thus raising the overall sum much higher. In the legal perspective, the card holders' own responsibility (omavastuu in Finnish) limit ends at 150 euros of damage, and after that it is the banks responsibility to cover any damages. That is the scenario if the card holder has not personally terminated his or her card. If the card is terminated at the moment the card holder notices its gone missing etc. The banks responsibility starts.

So, what's the technical side to the story, why is it possible to use contactless payment even after the card has been terminated? The reason is in the chip of the bank card. The NFC antenna is imbedded in the chip of the bank card and still remains operational even after the termination of the card because it only uses NFC technology and does not need to verify and transactions or has a need for internet connection. This means that basically every time a user gets a new card and leaves the old card laying around it is a security hazard. Every missing card can be a security hazard as well. This is why all the banks always instruct the users to physically terminate the cards as well by cutting through the chip of the card with scissors thus making the chip un-operational.

This leads us into the other case of crowded trains. Now there are multiple stories of POS's being used and scanners being used to steal card information and to make small purchases to unaware commuters (as in the relay attack scenario described earlier). One of these stories was published by Iltalehti on the 2nd of February 2017, where a developer of a physical card protection device (wallet) Timo Äärinen demonstrates how to easily scan the card information from a victim in a crowded area. In all simplicity skipping the

technical aspects the attack is done very similarly to relay attack where the victims card is scanned and the data processed with a mobile phone application. The interesting difference is that Pekka Nummela the team leader in OP from the previous news story argues that “it is not possible to find out the CVC/CVV number with these scamming methods” (Pekka Nummela Oululehti 2016). Clearly indicating that NFC is not a security risk in card information scanning. And this seems to be the popular opinion of bank representatives in general judging by comments in other stories and also in VISA’s official web page as well (Visa 2017). But in the Iltalehti story Timo Äärinen shows that it is simple to find out the security codes (CVV/CVC) with an app that tests the options one by one. To be fair there are only 1000 possibilities for the security code since the CVV/CVC number is a three-digit number. The danger lies in the fact that a lot of these attacks can be automated thus denying the bank representatives claims about that the attacks aren’t convenient for the attackers because of the effort to profit ratio. The danger is also the fact which a security manager at Nixu Niki Klaus claims “the user has no possibility to know whether his card has been scanned or not” (Iltalehti 2017). There are some possibilities to prevent falling a victim and one is to purchase or manufacture a physical protection around the card using tinfoil or making the purchase from any web store that sells the products such as: Lompakkoshop.fi (http://www.lompakkoshop.fi/lompakot/rfid-suojattu-lompakot.html).

(Figure 24 a NFC scanning protected metal case wallet from lompakkoshop.fi)

Discussion

5.9 Discussion and conclusions

It would seem obvious that there are some known and some unknown security threats in the field of NFC payment as the study and the multiple cases and studies would indicate. The study shows that the security threats that the providers of the NFC payment devices and services tell on their web sites (Nordea 2017) are merely the tip of the ice berg as a figure of speech out of all the possible security threats there are. It is also a valid assumption that the developers of security threats or attacks work faster paced than the people working on making NFC more secure. This can be said even though as some of the cites from the previous studies show; that there are computer scientists that also try to find vulnerabilities in order for the security personnel to be able to work on them and to improve the security of NFC (Charlie Miller, J. Vila & Rodriguez).

Now one thing that cannot be stated as a 100% fact, but an assumption that I can confidently hint towards is that; not all security threats are being made aware to the consumers. This claim is supported by the multiple bank personnel interviews on the cases gone through on this thesis i.e. saying that scenario A is impossible even though there's a clear report that scenario A has happened, and only stating the information that is available on any banks web site like in the case of Pekka Nummela from Osuuspankki claiming that scanning the bank card details is useless for the attacker because there's no way to find out the CVV/CVC numbers and Timo Äärinen showing, just how it actually is possible. Also as my survey study indicated, not that many people think that the NFC payment method is bullet-proof or even relatively safe. Out of all the 58 people that answered my survey I found out that 89% use NFC Payment with the bank card, one of the most hazardous devices and that the most common frequency of use was 1 – 6 times a week. Out of the 58 people almost 38% thought that the security of a portable POS is not as safe as a static POS, even though there wasn't an option to explain why. Later studies indicated that the news stories, also gone through in the cases in the thesis have had an impact on the answers with a high probability. This also mirrored to the fact that approximately 29% of the answerers thought of NFC payment to be relatively or very unsecure. And the highest risk scenario for the consumer was the misuse of a stolen card. Even though the banks websites state that the POS will ask the Pin-code of the card after making a couple of NFC Payments thus limiting the maximum damage to approximately 75€ instead of the other option if one's card details get copied and the victim could have his or her whole account drained.

Considering the results of the thesis it's possible to make the correlation between the consumer's trust in the service, the information available on the banks websites, the news stories and the studies. It would seem that there has been too many news about the security threats compared to what service providers inform that the consumers trust on the security of NFC payment is not that high, nor it in my opinion should be. This is just my opinion but I feel it could be because as a product and a service, NFC payment is new in Finland (first NFC Payment bank cards came available in 2013, korttiturvallisuus.fi), and has been lobbed and promoted so fiercely that the benefits of the fine service have overshadowed the security threats there are in the public and in the service providers eye. Whether the neglecting of the studies that indicate the security threats have been intentionally gone unseen or not, is something that would need further investigating.

To the question: what is the future of NFC payment? I would guess that the technology will be more and more common on mobile devices in the future. And there are many reasons why I think so. First; the possibility of MasterCard and Visa to become just service providers and eliminate the need to produce plastic, physical cards to customers would be a noticeable cut in expenses thus making it possible for the profit to be further directed to shareholders, or to develop the business and services. Even though the manufacturing expenses of a single bank card is not that high (0.50 US) (Finance Buzz 2016) there are over 1 billion bank cards manufactured every year in the United States alone (Finance Buzz 2016) making the savings of the expenses grand. The other reason why I predict such trend is that the traditional bank card is more vulnerable for attacks than a mobile phone, which can have a physical and a digital virus security and a firewall. It will indeed be interesting to see how the technology develops.

5.10 Follow-up Research & Possible topics

I think that especially since NFC payment is already relatively widely used in Finland that it would very beneficial to further examine the security threats and aggressively bring the facts to public knowledge. I don't think that there should be any limitations made to the expanding use of NFC as a payment method mainly because compared to pin code payment and the use of magnetic strip it is the better option, but just making people aware would help to decline the misuse statistics. For example, when looking on the case of relay attacks previously on this thesis, it's obvious that using a phone case with a bank card slot is a security threat of which many don't know anything about.

So, all-in-all there should be separate further research on the security threats on the technical side and there should be a further separate research, maybe in the form of surveys

or questionnaires like the one I conducted but in a much larger scale. That way the two researches would benefit of each other's results thus improving the security and the awareness of the end consumer. And I think that those are the two most obvious directions where to expand this study. On the technical side, many of the experiments that I cited were conducted in laboratory environments so it would be also good to experiment on actual scenarios with modern devices. It would seem that the attacks do work though as stated in the news stories. Basically, my thesis covers a bit of both sides of the research but it would be beneficial to have two separate researches as well.

Then again for the not so faint hearted there could lay a research on the honesty and informing policies of the service providers, but that is more of a job for a journalist. For the possible topics, there could simply be a research of practical NFC attacks, theoretical NFC attacks and both done to multiple devices. And on the theory side; The current awareness of NFC threats of the end user or just a trust factor analysis of the end users titled, Does the consumer trust in NFC security. The latter would be really beneficial for marketers and campaign workers I'm sure, since my study already indicated that the trust is not that high.

5.11 Thesis evaluation & Working methods

When I chose the topic for this thesis I had the image in mind that I wanted to conduct such studies that I cited in the thesis later. It quickly came apparent that the costs without a sponsor and the timetable would've proved to be too challenging so the focus point shifted a bit, but in my opinion not to worse. As I studied the security threats there are and the statistics and information about the successful attacks it came to me as a shock at first that why wasn't I aware of these factors, and the question also came to my mind that if I'm not aware of these threats how about the consumer of the service. I thought that surely since I work in banking my knowledge should exceed the knowledge of a person not in the industry, thus raising the urge to conduct a survey research. The amount of knowledge I gained in the process of conducting this thesis is so great that I will continue to work amongst NFC technology as a hobby, for example I have ordered my own devices and aim to improve the security of NFC furthermore. Overall I am really satisfied on the fact that I chose NFC Payment and security threats as my topic, for I had a great interest towards subject beforehand and now I know a lot more than the average person, and this also gives me an advantage in my career as well since in hours I have worked on the subject more than an average worker at say my workplace. Whether my thesis brings value to any company in any field of business remains to be seen, but I can proudly present my knowledge and my piece of work if an opportunity rises.

In any other way rating or reviewing my own thesis is troublesome for me since I have a really objective view on the piece of work. I'm also as a reviewer hard on myself, and I have a motto that everything can always be improved. So as neutrally as I can I would say that my thesis is slightly above average but wouldn't fit the bill of receiving any honours for even I feel that I could have researched a bit better and a bit further. Overall I think that the structure is simple and clear and that it supports the overall idea of the thesis. I think that all the chapters are necessary and no piece of information is useless. In a way if I'd have to say one developing point or a con in this thesis it would be that sometimes it was hard to stay in scope, because so many i.e. technological sides could've been gone through in much higher detail, but I think I managed well to keep everything relevant.

As for my working methods, I feel that my working style was intensive and independent. Intensive because I work best under a bit of pressure, this time provided by deadlines and my challenging schedule. And independent because of my status of full time employment, which meant that me and my thesis advisor communicated mostly via email and that I didn't need guidance in any of the thesis process phases like studying, writing etc. Overall I feel that this method of working suited me the best and all the praises for it was made possible.

References

Nordea henkilöasiakkaat, kortit, lähimaksaminen: Readable at: https://www.nordea.fi/henkiloasiakkaat/paivittaiset-raha-asiat/kortit/lahimaksaminen.html Read/Visited: 8.2.2017

Nordea, Q&A about contactless payments : Readable at: https://www.nordea.fi/en/personal-customers/everyday-finances/cards/frequently-asked-questions-contacless-payment.html#faq=Lahimaksaminen+103897 Read/Visited: 8.2.2017

Nordea, available cards for private customers: Readable at: https://www.nordea.fi/henkiloasiakkaat/paivittaiset-raha-asiat/kortit/ Read/Visited: 8.2.2017

Weebly 2017, NFC technology overview: readable at: http://nfc-tunniste.weebly.com/nfc-tekniikkaa.html Read/Visited: 8.2.2017

Apple 2017, Apple Pay: Readable at: http://www.apple.com/apple-pay/ Read/Visited: 8.2.2017

Tech Advisor 2015 / Matt Egan 2015, What is NFC? Uses of NFC, Readable at: http://www.pcadvisor.co.uk/how-to/mobile-phone/what-is-nfc-how-nfc-works-what-it-does-3472879/ Read/Visited: 9.2.2017

Tech Radar 2015, by Cameron Faulkner, what is NFC? Everything you need to know, readable at: http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410 Read/Visited: 9.2.2017

Google patent registry 1983, Portable radio frequency emitting identifier, readable at: https://www.google.com/patents/US4384288 Read/Visited: 9.2.2017

https://epxx.co/artigos/nfc_en.html Read/Visited: 9.2.2017

EPXX, Introduction to NFC (Near Field Communication) technology, readable at: http://nfc-forum.org/about-us/ Read/Visited: 9.2.2017

Ilta-Sanomat 2016: Viinarannekkeesta löytyi virhe: Maksaako uhri varkaan kaljat? Readable at: http://www.is.fi/taloussanomat/art-2000001917457.html Read/Visited: 16.3.2017

Harry Sintonen 2016, Vakava turvauhka AfterPay-rannekkeissa, readable at: https://sintonen.fi/advisories/afterpay-ranneke.txt Read/Visited: 16.3.2017

Harry Sintonen 2016, Vakava turvauhka AfterPay-rannekkeissa, readable at: https://sintonen.fi/advisories/afterpay-bracelet.txt Read/Visited: 16.3.2017

Tekniikka Talous 2015, Luottokorttitietojen varastamiseen riittää pelkkä taskussa oleva puhelin - Tutkijat esittelivät tekniikan, readable at: http://www.tekniikkatalous.fi/tekniikka/2015-06-11/Luottokorttitietojen-varastamiseen-riitt%C3%A4%C3%A4-pelkk%C3%A4-taskussa-oleva-puhelin---Tutkijat-esitteliv%C3%A4t-tekniikan-3323304.html Read/Visited: 16.3.2017

Security Affairs / Pierluigi Pagani 2015, NFC attack can steal your credit card information, readable at: http://securityaffairs.co/wordpress/37667/hacking/nfc-attack-credit-card.html Read/Visited: 16.3.2017 & Read/Visited: 6.4.2017

J. Rodriguez & Jose Vila 2015, Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited, readable at: https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2014/12/WHITEPAPER-Relay-Attacks-in-EMV-Contactless-Cards.pdf Read/Visited: 16.3.2017

Infosec 2013, Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema, readable at: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema Read/Visited: 28.3.2017

Iltalehti 2016, LÄHIMAKSUKORTILLA HUIJATUKSI - NÄIN SE TOIMII, VARO, readable at: http://www.iltalehti.fi/iltvuutiset/201603080083600_v0.shtml Read/Visited: 6.4.2017

Stackoverflow 2013, can android phone act as tag, readable at: http://stackoverflow.com/questions/6138077/can-an-android-nfc-phone-act-as-an-nfc-tag Read/Visited: 6.4.2017

Korttiturvallisuus.fi, lähimaksaminen, readable at: https://www.korttiturvallisuus.fi/Kaupassa/Lahimaksaminen/ Read/Visited: 6.4.2017

Make use of, by Joel Lee 2014: How Does A Drive By NFC hack work? readable at: http://www.makeuseof.com/tag/drive-nfc-hack-work/ Read/Visited: 6.4.2017

Tampereen teknillinen yliopisto 2014 by Jenna Lehtimäki, Near Field Communication ja sen tietoturvaongelmat, readable at: https://wiki.tut.fi/Tietoturva/Tutkielmat/NFC-tietoturva Read/Visited: 6.4.2017

VISA 2017, FAQ Contactess payment, readable at: https://www.visa.fi/fi/maksa-visalla/lahimaksaminen/yleisimpia-kysymyksia Read/Visited: 6.4.2017

Iltalehti 2017, Satojentuhansien pankkikorttien tiedot vaarassa lähimaksujen takia - katso videolta miten, readable at: http://www.iltalehti.fi/uutiset/201702062200064688_uu.shtml Read/Visited: 6.4.2017

Oululehti 2016/ OP Pekka Nummela, Lähimaksu onnistuu, vaikka kortti olisi suljettu, readable at: http://www.oululehti.fi/uutiset/lahimaksu-onnistuu-vaikka-kortti-olisi-suljettu-6.255.108044.caa5664241 Read/Visited: 6.4.2017

MTV 2016, Lähimaksuominaisuudessa piilee vaara – mies vei rahaa ihmisten pankkikorteilta junassa, readable at: http://www.mtv.fi/uutiset/ulkomaat/artikkeli/lahimaksuominaisuudessa-piilee-vaara-britanniassa-mies-vei-rahaa-ihmisten-pankkikorteilta-junassa/5745558 Read/Visited: 6.4.2017

Charlie Miller 2012, Exploring the NFC Attack Surface, readable at: https://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf Read/Visited: 6.4.2017

Finance Buzz 2016, HOW MUCH DOES A CREDIT CARD COST? readable at: http://financebuzz.io/finance-credit-card-cost Read/Visited: 16.4.2017

Figures used in the thesis:

Figure 1: http://cdn.dynatracker.de/blog/kostenlose-kreditkarte-der-dkb-folgt-neuem-trend-jetzt-auch-kontaktlos-bezahlen-15-595.png

Figure 2: https://www.sv-oy.fi/wp-content/uploads/iWL250-card3-e1442229115537.jpg

Figure 3: http://www.lansi-savo.fi/sites/default/files/styles/flexslider_full/public/images/news_item/kortti_laite_ja_aallot.jpg?itok=K1GNGM6H

Figure 4: https://www.nordea.fi/Images/58-161875/kortit-debit-2017-186x120.jpg

Figure 5: https://www.nordea.fi/Images/58-161877/kortit-credit-2017-186x120.jpg

Figure 6: https://www.nordea.fi/Images/58-161771/kortit-electron-2017-186x120.jpg

Figure 7: https://www.nordea.fi/Images/58-161876/kortit-gold%20kuva-2017-186x120.jpg

Figure 8: Own screenshot from OnePlus 3T phone, not available in the internet

Figure 9: http://nfc-tunniste.weebly.com/uploads/1/8/1/2/1812051/_1375297774.png

Figure 10: https://en.wikipedia.org/wiki/Near_field_communication#/media/File:NFC_Protocol_Stack.png

Figure 11: http://blog.protocolbench.org/wp-content/uploads/2013/11/ISO-Layer_Smart-Card.png

Figure 12: http://docplayer.net/40299305-Experiences-on-nfc-relay-attacks-with-android-virtual-pickpocketing-revisited.html

Figure 13: https://i0.wp.com/securityaffairs.co/wordpress/wp-content/uploads/2015/06/NFC-attack.jpg?w=606

Figure 14: A screenshot from the pdf: https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2014/12/WHITEPAPER-Relay-Attacks-in-EMVContactless-Cards.pdf

Figure 15: http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/061713_1855_NearFieldCo4.jpg

Figure 16: https://www.slideshare.net/the_netlocksmith/defcon-2012-nearfield-communicationrfid-hacking-miller

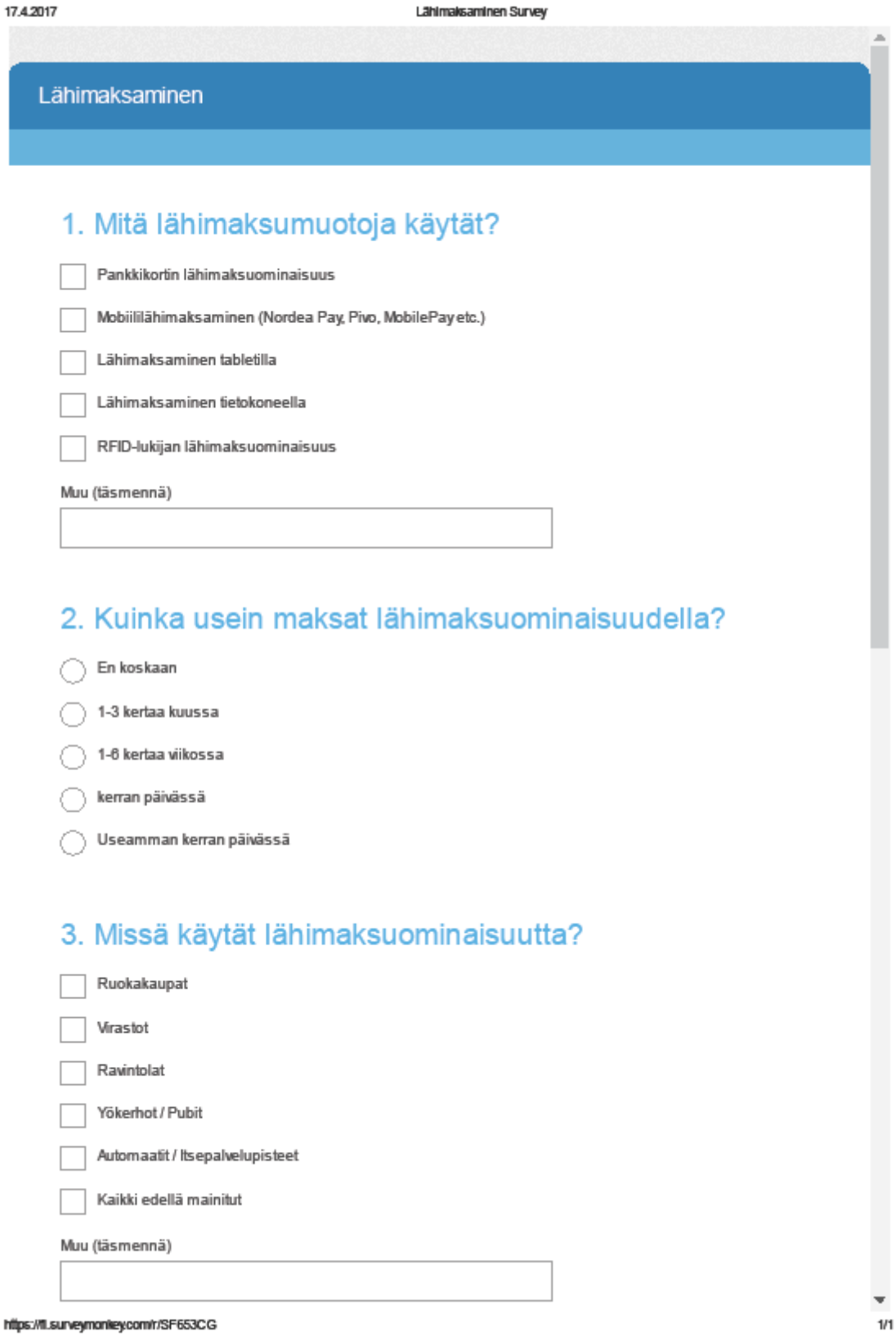
Figures 17 – 22: All from the survey monkey survey, available in the appendices.

Figure 23: https://crop.kaleva.fi/fUZjEzRgiiaOwl3wXb3794bXeJ8=/894x0/smart/http%3A//kuvat.kaleva.fi/default/365f3588-54d4-11e6-ba8f-22000a239905/xlarge-16428510.jpg

Figure 24: http://www.lompakkoshop.fi/media/catalog/product/cache/23/image/476x476/9df78eab33525d08d6e5fb8d27136e95/t/h/thin-king-cardcase_1.jpg

Appendices

Appendix 1. The survey and the Survey answers



17.4.2017 Lähimaksaminen Survey

Lähimaksaminen

1. Mitä lähimaksumuotoja käytät?

- [ ] Pankkikortin lähimaksuominaisuus
- [ ] Mobiililähimaksaminen (Nordea Pay, Pivo, MobilePay etc.)
- [ ] Lähimaksaminen tabletilla
- [ ] Lähimaksaminen tietokoneella
- [ ] RFID-lukijan lähimaksuominaisuus

Muu (täsmennä)

2. Kuinka usein maksat lähimaksuominaisuudella?

- ( ) En koskaan
- ( ) 1-3 kertaa kuussa
- ( ) 1-6 kertaa viikossa
- ( ) kerran päivässä
- ( ) Useamman kerran päivässä

3. Missä käytät lähimaksuominaisuutta?

- [ ] Ruokakaupat
- [ ] Virastot
- [ ] Ravintolat
- [ ] Yökerhot / Pubit
- [ ] Automaatit / Itsepalvelupisteet
- [ ] Kaikki edellä mainitut

Muu (täsmennä)

https://fi.surveymonkey.com/r/SF653CG 1/1

4. Koetko että maksupäätteen mallilla (kiinteä/kannettava) on väliä turvallisuuden kannalta?

- ◯ Kyllä
- ◯ Ei

5. Kuinka turvallisena pidät lähimaksamista?

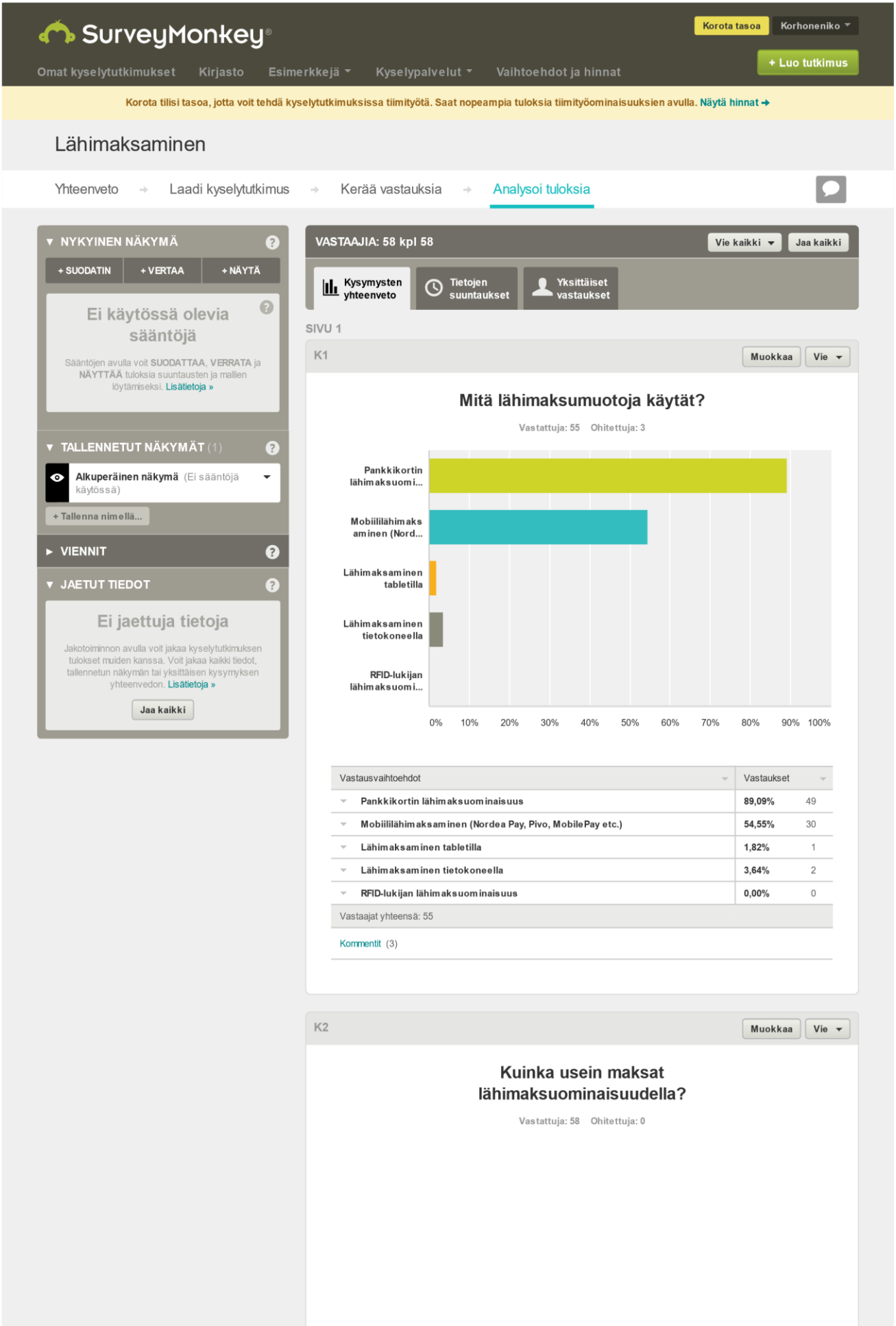
- ◯ Erittäin turvallisena
- ◯ Melko turvallisena
- ◯ Hieman epäturvallisena
- ◯ Erittäin epäturvallisena

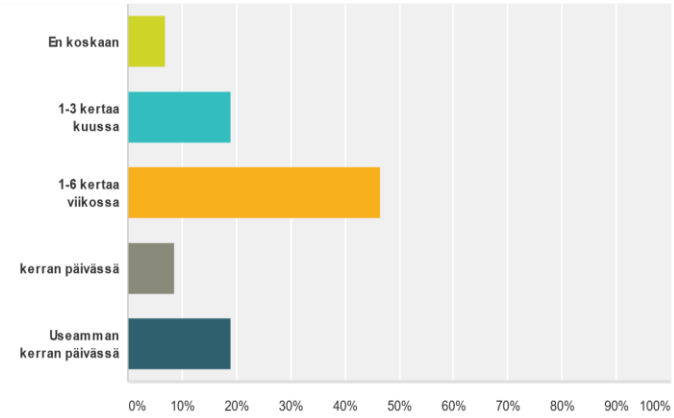
6. Mitä pidät lähimaksuominaisuuden suurimpana turvallisuusriskinä?

- ◯ Kortin tietojen kopiointi (esim. lukijalla lähietäisyydeltä)
- ◯ Varastetun kortin väärinkäyttö (useat n.25€ ostokset)
- ◯ Haittaohjelmat ja virukset (koskee laitteita)

Muu (täsmennä)

Valmis


SurveyMonkey
Korota tasoa
Korhoneniko
Omat kyselytutkimukset
Kirjasto
Esimerkkejä
Kyselypalvelut
Vaihtoehdot ja hinnat
+ Luo tutkimus
Korota tilisi tasoa, jotta voit tehdä kyselytutkimuksissa tiimityötä. Saat nopeampia tuloksia tiimityöominaisuuksien avulla. Näytä hinnat
Lähimaksaminen
Yhteenveto
Laadi kyselytutkimus
Kerää vastauksia
Analysoi tuloksia
NYKYINEN NÄKYMÄ
+ SUODATIN
+ VERTAA
+ NÄYTÄ
Ei käytössä olevia sääntöjä
Sääntöjen avulla voit SUODATTAA, VERRATA ja NÄYTTÄÄ tuloksia suuntausten ja mallien löytämiseksi. Lisätietoja »
TALLENNETUT NÄKYMÄT (1)
Alkuperäinen näkymä (Ei sääntöjä käytössä)
+ Tallenna nimellä...
VIENNIT
JAETUT TIEDOT
Ei jaettuja tietoja
Jakotoiminnon avulla voit jakaa kyselytutkimuksen tulokset muiden kanssa. Voit jakaa kaikki tiedot, tallennetun näkymän tai yksittäisen kysymyksen yhteenvedon. Lisätietoja »
Jaa kaikki
VASTAAJIA: 58 kpl 58
Vie kaikki
Jaa kaikki
Kysymysten yhteenveto
Tietojen suuntaukset
Yksittäiset vastaukset
SIVU 1
K1
Muokkaa
Vie
Mitä lähimaksumuotoja käytät?
Vastattuja: 55 Ohitettuja: 3
Pankkikortin lähimaksuomi...
Mobiililähimaksaminen (Nord...
Lähimaksaminen tabletilla
Lähimaksaminen tietokoneella
RFID-lukijan lähimaksuomi...
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Vastausvaihtoehdot
Vastaukset
Pankkikortin lähimaksuominaisuus 89,09% 49
Mobiililähimaksaminen (Nordea Pay, Pivo, MobilePay etc.) 54,55% 30
Lähimaksaminen tabletilla 1,82% 1
Lähimaksaminen tietokoneella 3,64% 2
RFID-lukijan lähimaksuominaisuus 0,00% 0
Vastaajat yhteensä: 55
Kommentit (3)
K2
Muokkaa
Vie
Kuinka usein maksat lähimaksuominaisuudella?
Vastattuja: 58 Ohitettuja: 0

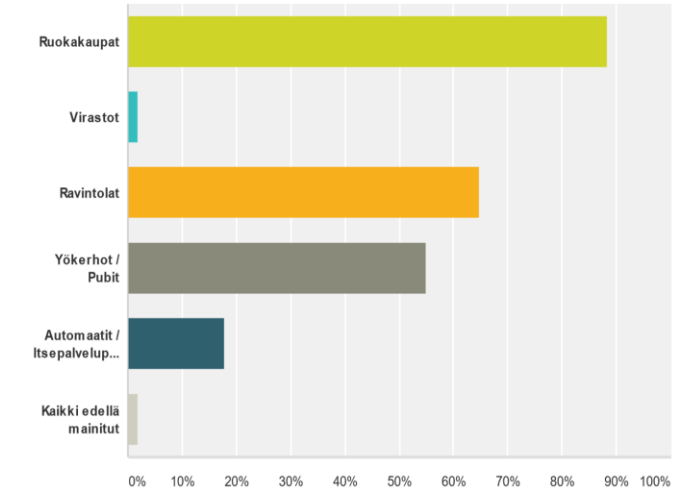


Vastausvaihtoehdot	Vastaukset	
En koskaan	6,90%	4
1-3 kertaa kuussa	18,97%	11
1-6 kertaa viikossa	46,55%	27
kerran päivässä	8,62%	5
Useamman kerran päivässä	18,97%	11
Yhteensä		58

K3 Muokkaa Vie

Missä käytät lähimaksuominaisuutta?

Vastattuja: 51 Ohitettuja: 7



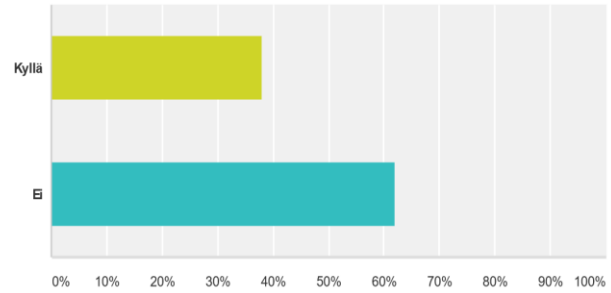
Vastausvaihtoehdot	Vastaukset	
Ruokakaupat	88,24%	45
Virastot	1,96%	1
Ravintolat	64,71%	33
Yökerhot / Pubit	54,90%	28
Automaatit / Itsepalvelupisteet	17,65%	9
Kaikki edellä mainitut	1,96%	1
Vastaajat yhteensä: 51		

Kommentit (10)

K4 Muokkaa Vie

Koetko että maksupäätteen mallilla (kiinteä/kannettava) on väliä turvallisuuden kannalta?

Vastattuja: 58 Ohitettuja: 0

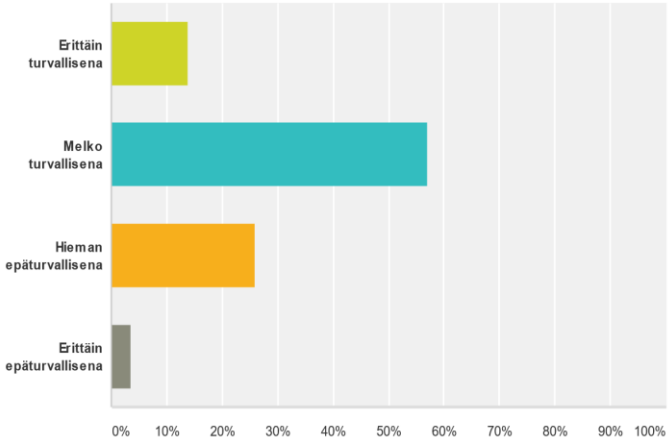


Vastausvaihtoehdot	Vastaukset	
Kyllä	37,93%	22
Ei	62,07%	36
Yhteensä		58

K5 Muokkaa Vie

Kuinka turvallisena pidät lähimaksamista?

Vastattuja: 58 Ohitettuja: 0

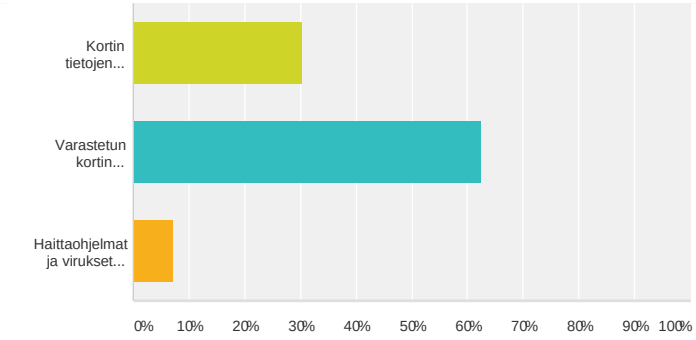


Vastausvaihtoehdot	Vastaukset	
Erittäin turvallisena	13,79%	8
Melko turvallisena	56,90%	33
Hieman epäturvallisena	25,86%	15
Erittäin epäturvallisena	3,45%	2
Yhteensä		58

K6 Muokkaa Vie

Mitä pidät lähimaksuominaisuuden suurimpana turvallisuusriskinä?

Vastattuja: 56 Ohitettuja: 2



Vastausvaihtoehdot	Vastaukset	
Kortin tietojen kopiointi (esim. lukijalla lähietäisyydeltä)	30,36%	17
Varastetun kortin väärinkäyttö (useat n.25€ ostokset)	62,50%	35
Haittaohjelmat ja virukset (koskee laitteita)	7,14%	4
Yhteensä		56

Kommentit (2)