Security of RFID-based technology

Tommi Hakamäki
Seinäjoki University of Applied Sciences
School of Technology
Seinäjoki, Finland
tommitapanihakamaki@gmail.com

Heikki Palomäki
Seinäjoki University of Applied Sciences
School of Technology
Seinäjoki, Finland
heikki.palomaki@seamk.fi

Abstract— **RFID-based access control systems and contactless payment cards are used in various applications in people's everyday lives. Nevertheless only a few know how this technology actually works. The information security of access control systems has not been discussed in public even though several different hacking methods for the systems have been developed and published. Implementation of contact-less payment cards has received similar attention, but media attention has still remained rather marginal.**

This article presents the basics of RFID-technology, the methods of information security and the several different hacking methods that have been published in one form or another. The information security of contactless payment cards will also be covered and the current security status will be assessed.

The main security problem is that existing technology is too old and new systems are made to be compatible with old ones continuing the poor security practices. Because the protocols are following public standards, the methods are known to hackers. Security risks are increasing because of mobile phones with NFC-interfaces with free NFC-reader applications. However, the technology is still mostly secure because the problems are mostly unknown.

As a result, the insecure state of RFID-based access control systems and of contactless payment cards has been processed. Also the possible causes for the current situation were considered.

Keywords— RFID; NFC; access control; contactless payment cards

I. Introduction

The use of the RFID based systems and NFC (Near Field Communication) contactless payment card technology has increased continuously during the last ten years. The usage of access control systems has become more common in academies, markets, companies and in public administrations, such as hospitals, health centres, police- and fire stations. In many different control systems, the RFID technology transmits important private or publicly secure data. For example contactless NFC payment cards have been noticed widely. The function of this technology is to offer novel, faster and especially a more secure way to execute daily payments and purchases.

The manufacturers and service providers guaranteed the security and reliability of their RFID and NFC systems. The future committee of Finland parliament published a bulletin in year 2011, in which was stated that nobody had succeed in copying the RFID tags (identifiers) used in access control systems [31]. Nevertheless before this same year there had been presented many different ways to copy and use unauthorized RFID based tags. The information on data security problems differs very greatly depending on the source of the information. Also, it is often insufficient.

II. State of the Art

A. History

The RFID and NFC technology are based on primary and secondary surveillance radars created and designed for military use. It consists of an earth station and a secondary radar transponder installed in the warplane or the ship. Second radar system was the first example of the modern RFID system [32, pp. 45-47].

The forerunner of the modern passive RFID tags was the EAS (Electronic Article Surveillance) anti-theft system, developed and taken into use in the 1950's and 1960's [29]. In the year 1973 Mario Cardullon patented the first active identifier which used digital memory. This same year Charles Walton patented the first RFID system based on the passive identifier [32, pp. 49-51].

In the beginning of 1990's, engineers at IBM developed and patented a RFID system using 0.3–3 GHz:n microwave frequencies. Between the years 1999 and 2003 Auto-ID center gathered over 100 large companies to sponsor and develop two communication protocols and the EPC numbering system [29].

B. Features

The RFID system consists of at least of three separate devices: RFID identifier, reader and control system. The communication between the identifier and the reader functions as a contactless inductive connection using LF and HF frequency bands, with an oscillating magnetic field. Using UHF and microwave frequency bands the communication uses normal radio waves. The most used frequency bands are LF, HF and UHF. The used frequencies are defined in more detail with country-specific variations. The aim is to create common frequencies to be used in the global standardization [13, pp. 6-26].

Table 1 shows these frequency bands and frequency limits.

Table 1: Used RFID frequencies [7].

Frequency bands	Most used frequencies
LF (low frequency)	125 – 134 kHz
HF (high frequency)	13.56 MHz
UHF (ultra high frequency)	860-960 MHz

Today, after nearly a century after its invention, RFID technology has already been utilized worldwide and there are a huge number of applications. For a normal customer the technology can seem novel and highly developed, but the case is about rather old technology. Only the applications are new [34].

Figure 1 shows some applications using RFID technology.

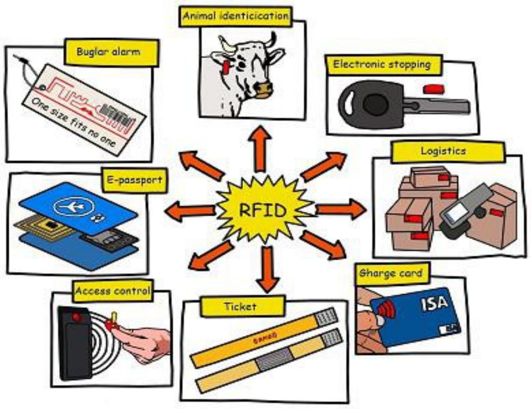


Figure 1. Application examples of RFID technology

III. Function

A. Standards

The standardization of RFID technology is not yet ready as a whole. The only standard ready today is EPC global UHF Gen2 V1, which includes passive RFID systems using UHF frequencies i.e. UHF RFID identifiers and readers. The most important organizations in standardizations are ISO, IEC and EPC-global. Some examples are shown in Table 2. NFC technology is based on RFID and it uses also ISO and IEC-standards [18].

The features of payment cads using integrated circuitry are defined by EMV standardization. EMV standard also defines features and demands for contactless payment cards i.e. NFC cards [11].

Table 2: Examples of ISO-standards [13]

Standard	Definition
ISO 11784 ISO 11785 ISO 14223	Data content, communication and air interface of identifiers used in animal husbandry
ISO 10536	Identifiers using 4.9152 MHz frequency and maximum 1 cm reading distance
ISO 14443	Identifiers using 0–10 cm reading distance
ISO 15693	Identifiers using 13.56 MHz frequency and 0–1m reading distance
ISO 18000	Air interface and obligatory commands of identifiers using separate frequencies

B. RFID identifier

The identifier is the user part of the RFID or NFC system. The identifier or tag consists in minimum of antenna, microcontroller and some other demanded electronic components. Depending on the application and type, the identifier might also include extra microcontrollers, power sources, sensors and passive electronic components [32, pp. 50-74].

The identifiers can be passive, half-passive or active. The passive RFID or NFC identifiers are the most common and are low-cost used in many different variations. This kind of identifiers gets energy from the reader and doesn't include an internal power supply. Using readers, the normal working distance is some centimetres, but it can be over 10 m. In some cases the distance can be as much as 100 m [4].

The size of one of the smallest passive RFID identifiers is 0.05x0.05mm. Hitachi released it in 2007 [2]. Figure 2 shows the size of the Hitachi's identifier.

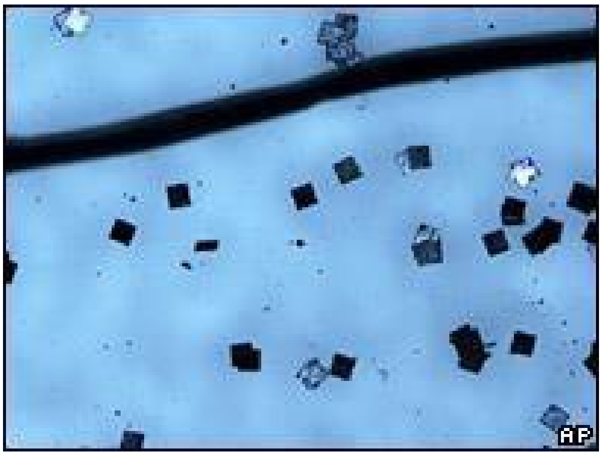


Figure 2. The size of the Hitachi RFID identifier compared with a hair [2]

The half-passive identifiers include the internal power source which is used only in the internal operations of the microcontroller i.e. encryption and data processing.

The active identifier includes a power supply and a transmit circuit. The read distance is longer with these features [28]. Figure 3 shows different ways of encapsulating identifiers.

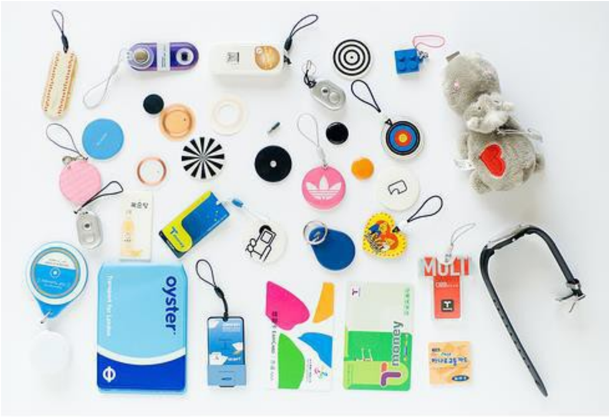


Figure 3. Different RFID identifiers and encapsulations [1]

NFC identifiers use the same basic features as the passive RFID identifiers. NFC technology is basically more specified part of RFID, also it is used in some mobile devices. It does not offer better data protection, unless the mobile device itself is used as an identifier. NFC also uses different data format. The most visible and common application for NFC identifiers is contactless payment cards [6]. Figure 4 shows X-ray photos of some contactless payment cards.

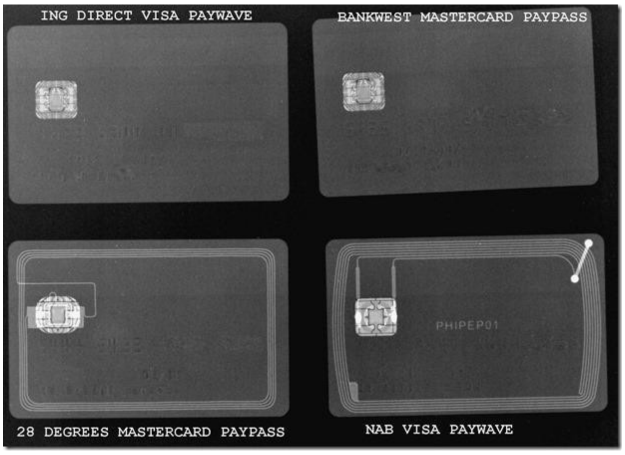


Figure 4. X-ray photos of four different NFC payment cards. [22]

The function of the microcontroller in the identifiers is mostly for data acquisition. The same chip converts AC voltage from the antenna to DC voltage. In passive identifiers, all data and power needed by the microcontroller comes via the antenna. Half passive and active identifiers have an internal power supply [13].

Figure 5 shows the internal functions of the microcontroller chip including the radio part and data acquisition.

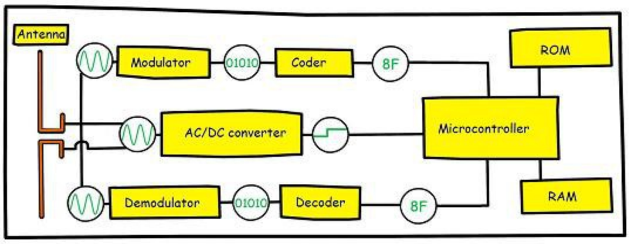


Figure 5. Functional block diagram of a microcontroller

C. RFID reader

The reader device consists of two parts: transponder (i.e. transmitter and receiver) and control electronics. The most important function of the transponder is to generate the required energy for the identifier via radio waves and so activate the identifier. The other function is to receive and demodulate data from the identifier and relay the data to the control system. In the opposite direction the transponder receives data from the control system and modulates and transmits it to the identifier [13, pp. 309-317]. Figure 6 shows an example of how the transponder processes data.

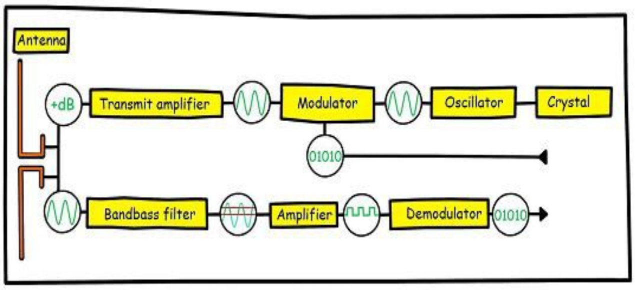


Figure 6. Data processing in a transponder

The communication bus between the reader and the possible control system can be for example Wiegand-wiring, RS232 or RS485 [13, pp. 316-317].

D. Control system

The control systems can be divided into two main groups depending on functionality: online or offline systems. The online system is a traditional mainframe system, where data is transmitted from the reader to the mainframe computer. In the offline system, the reader includes a list of used identifiers. The management of the identifiers is very different in these two systems. In the online systems identification management and permission control is centralized. In the offline systems modifications are made by programming and reprogramming the identifier or manually updating singular readers [13, pp. 357-359].

The contactless payment cards mostly use NFC technology. The control system, based on payments, is complex. The payment transaction of the contactless payment cards is similar to electronic cash cards. The transaction can be divided into 9 parts from card identification to the end of the transaction [10]. Figure 7 shows the payment transaction phases.

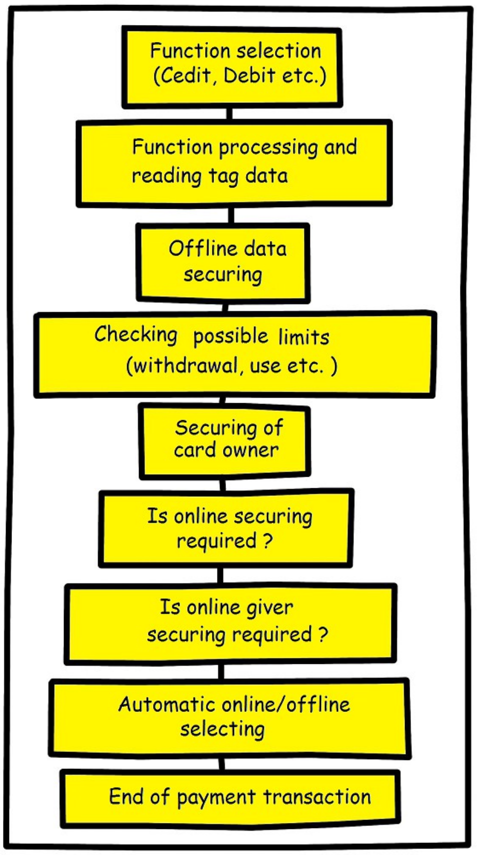

Function selection (Cedit, Debit etc.)
Function processing and reading tag data
Offline data securing
Checking possible limits (withdrawal, use etc.)
Securing of card owner
Is online securing required ?
Is online giver securing required ?
Automatic online/offline selecting
End of payment transaction

Figure 7. Payment transaction phases

E. Data structures

Data in the identifiers are divided into blocks. Size of these blocks is defined by used standardization. The blocks include different types of data and form a proper data structure. The most common data structures in RFID identifiers are Class-1 Gen-2 and Wiegand. The first mentioned data structure from EPC-global consists of four separate data blocks. The structure is planned especially for the needs of logistics industry [12]. Figure 8 shows the data structure of Gen 2.

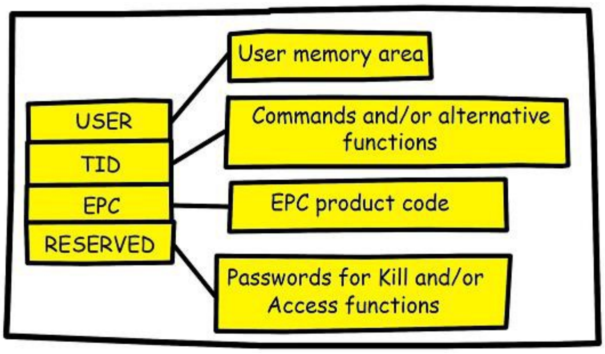

USER
TID
EPC
RESERVED
User memory area
Commands and/or alternative functions
EPC product code
Passwords for Kill and/or Access functions

Figure 8. EPC Gen 2 data structure

The Wiegand structure is very common in access control applications. The 26 bit data format is commonly available and simple to implement. Therefore it is one of the most used data format in access control systems [16]. Figure 9 shows one example of the data structure of Wiegand.

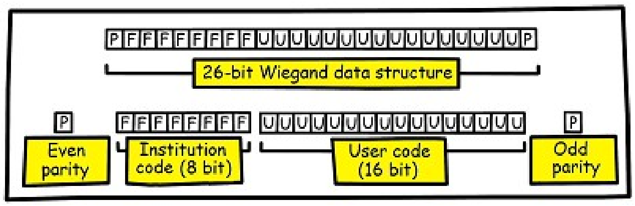


Figure 9. An example of 26 bit Wiegand data structure

NDEF structure, developed by NFC Forum, is used in NFC identifiers. NDEF consist of one or more data records shown in Figure 10 [23].

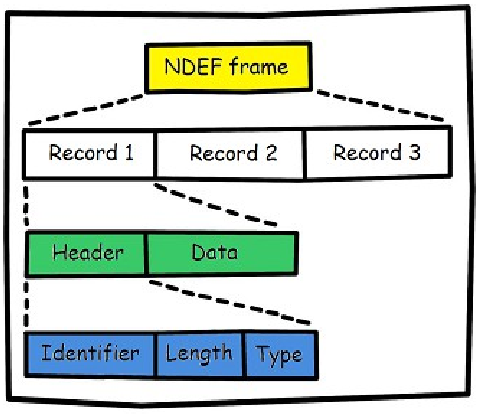


Figure 10. NDEF data structure

IV. Used data security

This chapter consist of data security methods used in RFID and NFC technology. Also, there are some example cases of hacking and utilization technics. The focus is especially on RFID technology used in access control systems and NFC technology used in contactless payment transactions.

A. Authentications

By authentications it is possible to ensure, that the identifier has the rights to the functions executed via the reader. If the application needs a higher security level, it is important also to authenticate that the reader also has the right to accept the identifier and to connect with the control system. This means that before any data is sent all the applications need to authenticate themselves to each other and after approved authentication data can be sent [19].

Authentication is often realized by the challenge-response method, in which the reader first transmits a randomly generated number sequence or the internal clock time. The identifier must then respond with answer that is encrypted or modified correctly. Challenge-response is defined in ISO 9798 standard for RFID based technology. The essential security feature is a predefined coding method in which the reader does not transmit any secure information to the identifier [19].

B. Encryption

It is possible to read the encryption key from the identifier, but it requires suitable laboratory instrumentation. With this it is possible to physically skim the controller chip layer by layer. The layers can be then analysed using a microscope and arranged to mathematic formulas [19]. This method was used to hack the encryption of the ***MiFare Classic*** microcontroller in 2008 [8].

Theoretically, it is possible to make RFID technology which is impossible to hack, but it requires high level features from the identifier and the reader. It means that this kind of system would require more powerful and high-cost microcontrollers [19].

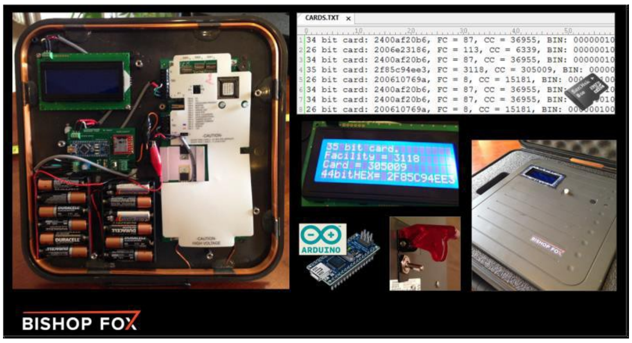
Encryptions aim in communication is that both transmitted and received data is encrypted. Encrypted data can be read only by using the encryption key. It can be predefined or it can be created for every case using the challenge-response method. If the identifiers transmitted data includes only the identification code, unauthorized reading doesn't result a big damage. But in identifiers which include important data, as in payment cards, strong encryption is needed. Therefore the identifier requires also a more powerful controller [19].

V. UNAUTHORIZED USE

In access control, the identifiers do not normally include any encryption or identification features because of costs. It means that the reader transmits the identification codes in a readable format, without security or encrypting [5].

The unauthorized reading of an identifier is possible by skimming i.e. by the $$grabbing method. In this case the person with an unauthorized reader must be very close to the identifier. With newly developed devices, long distance reading is also possible for some identifier types. Also, the size of the devices is decreasing following technology development [5].

The security consultant company ***Bishop Fox*** have published guides on how to build a long distance RFID reader. The device called ***Tastic RFID Thief*** consists of commonly available RFID reader connected with an Arduino microcontroller [3]. Figure 11 shows a ***Tastic RFID Thief*** device with a RFID reader.



CARDS.TXT

```
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
26 bit card: 2006e23186, FC = 113, CC = 6339, BIN: 00000010
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
35 bit card: 2f85c94ee3, FC = 3118, CC = 305009, BIN: 00000
26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 000   100
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN:       10
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN:      010
26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 00   00100
```

```
35 bit card.
Facility = 3118
Card = 305009
44bitHEX= 2F85C94EE3
```

Figure 11. Tastic RFID Thief [5]

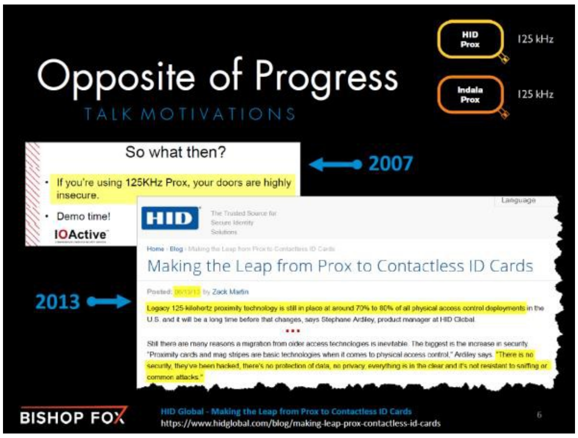
A. Hacking

To hack an identifier it means to convert the encrypted data in the identifier into a readable format.

The encryption methods of many RFID manufacturers have been hacked. One the best known case was in 2008 when ***Mifare Classic*** identifiers made by ***NXP Semi-conductors*** were hacked by German researchers and the white paper released to the public. This microcontroller is used widely in many applications and systems. The failure of the manufacturer was, that the encryption method was not updated after the publication in 1994. At this time the 48-bit encryption was still top notch technology [15].

In June 2013 the product manager of the company ***HID Global***, ***Stephany Ardillry*** wrote in her company blog, that the Legacy 125KHz series devices are no longer secure. All of the devices were encrypted and the users do not have any protection against unauthorized use in practice. She also wrote, that 70-80 percent of access control systems in the USA still use this same technology. The blog was later removed from the company's pages [5].

These above mentioned Legacy 125kHz series products were proven to be very vulnerable already in 2007 [27]. Figure 12 shows some publications about data security of ***Legacy 125kHz*** series technology.



Opposite of Progress

TALK MOTIVATIONS

So what then?

- If you're using 125KHz Prox, your doors are highly insecure.
- Demo time!

Making the Leap from Prox to Contactless ID Cards

Posted: 06/13/13 by Zack Martin

Legacy 125-kilohertz proximity technology is still in place at around 70% to 80% of all physical access control deployments in the U.S. and it will be a long time before that changes, says Stephane Ardiley, product manager at HID Global.

...

Still there are many reasons a migration from older access technologies is inevitable. The biggest is the increase in security. "Proximity cards and mag stripes are basic technologies when it comes to physical access control," Ardiley says. "There is no security, they've been hacked, there's no protection of data, no privacy, everything is in the clear and it's not resistant to sniffing or common attacks."

HID Global - Making the Leap from Prox to Contactless ID Cards
https://www.hidglobal.com/blog/making-leap-prox-contactless-id-cards

HID Prox
125 kHz
Indala Prox
125 kHz
2007
2013
IOActive
HID
The Trusted Source for Secure Identity Solutions
Language
Home · Blog · Making the Leap from Prox to Contactless ID Cards
BISHOP FOX
6

Figure 12. The hacking of 125kHz security technology [5]

B. *Unauthorized copying*

Unauthorized copying of an identifier means to hack and read unauthorized data from one identifier and copy the read data to another identifier.

In 2013 there was ***Black Hat USA*** conference, where ***Francis Brown***, the spokesman of the security consult company ***Bishop Fox***, presented a simple way to read, hack and copy the existing RFID systems. He also presented the main reason for it as: the lifetime of the system is 20 years or more, therefore the level of the data security does not fit the demands of today [5].

C. *Skipping the reading*

Skipping the reading means the use of the reader and the control system without using the identifier by accessing the wiring or electronics of the target system.

Most of the existing readers in security systems are using or can use communication method following Wiegand protocol and wiring between the reader and the control system. This is not the only protocol, but most used one [14].

It is possible to connect your electronics into the microcontroller in the reader; even inside the casing. This kind of device is for example ***Gecko***, presented by ***Zac Franken*** in 2007. Gecko is installed either inside the readers casing to the controller or to the wires going out from the reader. Gecko reads data after the installation and can reply recorded data sequences again by command, in this way faking the read event. The communication between the reader and the control system is often not encrypted following open Wiegand protocol. Not only RFID readers, but also most other access control readers use this same protocol i.e. iris scanners. The wires are not usually sabotage secured and the reader casings are not secured against unauthorized opening, therefore an unauthorized connection in the system is possible. It is rather difficult to update the Wiegand protocol with a better one, because all access control systems should also be updated to support the new format [35]. Figure 13 shows Frank Zetter's Gecko device.

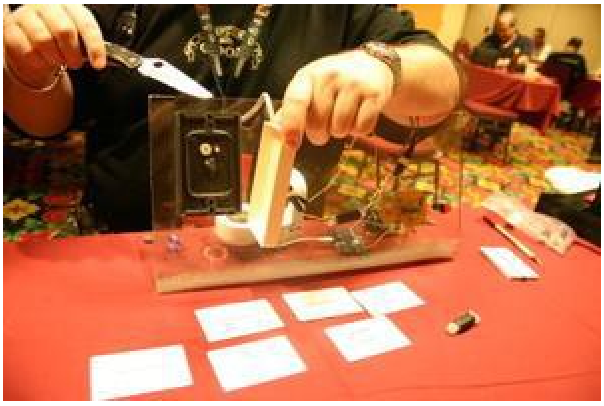


Figure 13. Gecko contacted with RFID reader [35]

D. *Exploitation of payment cards*

For example Danske Bank, OP-Pohjola and Nordea offer contactless payment cards based on NFC technology in Finland. These service providers had about one million NFC cards in use in December 2014. It means that every fifth Finn had a NFC payment card [17].

The number of NFC payment cards is assumed to increase especially, because many banks are adding this feature to payment cards as obligatory when updating cards: for example OP-Pohjola and Nordea [20].

NFC payment cards have become more common, because of higher usage security and faster payment transaction for transactions under 25€. Higher usage security means that it is no longer required to enter the PIN code before transaction, except in beginning and after some pre-set usage times. So nobody can observe the PIN code and misuse it [26] [25].

It is especially notable that the data security with NFC payment cards makes it more difficult to physically steal the card, because the PIN code is not known. In the other hand it is much simpler to electronically steal data from the NFC card. In May 2013 one Finnish cyber security company ***Nixu*** tested, is it possible to read data from a NFC payment card. The result was that they succeeded to read the card number, validity period and the name of the card holder in less than one second using a reader which costs about 20€. So the data in question is completely unprotected. Everyone can read it with the right kind of reader device. Also, they tested that with stolen data from the card it was possible to make online purchases. In online shops there is not the 25€ limit, as there is when using the card, so the criminal financial benefit can be very big [24].

The above-mentioned data security hole is not new, because even in one study in 2006 it was demonstrated that the first generation NFC payment cards has the same vulnerability as in the test by ***Nixu*** in 2013. The manufacturers planned to increase security for the next generation of cards already in 2006 by removing the holder's name from the data sent from card [30].

In the 2014 Eddie Lee developed a device configuration which is one of the most refined and novel devices, which captured data from NFC payment cards and exploited this data. This configuration requires two mobile phones with the NFC features. In the simple example one mobile phone using NFC reading feature was brought near the payment card. It collects all the needed data from the card. At the same time another mobile phone emulates the NFC payment card using the NFC feature near the payment terminal. The payment terminal sends an APDU request to the emulating mobile phone. This request is sent to the other phone via the internet and up to the payment card. The right answer from the payment card is transmitted back in the same way. So the payment was made using a payment terminal. With the same system it is possible to analyse the communication between phones and so decrypt and replay the functions of the NFC payment card [21]. Figure 14 shows the system communication developed by Lee.

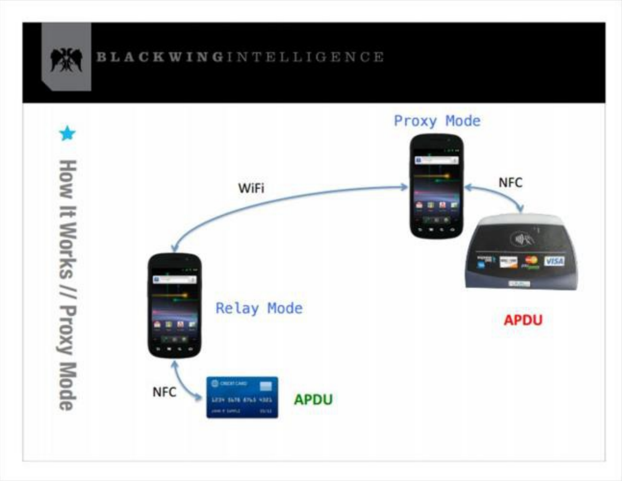


Figure 14. System communication by Lee [21]

IHS Technology presented in their publication how the use of the NFC features increases remarkable by the year 2018. 18.2% of all 1.5 billion mobile phones delivered is 2012 use NFC feature and by 2018 the amount increases to 64% [33]. Figure 15 shows delivered number of NFC mobile phones.

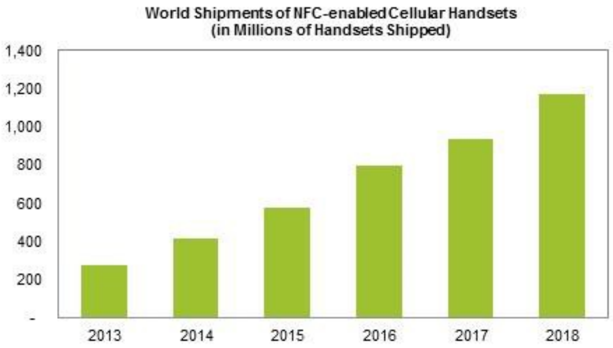


Figure 15. Delivered NFC mobile phones in the years 2013–2018 [33]

One of the most significant and advertised security features of NFC is the short reading distance. Researches have proven, that longer distances are also possible, but by using high-cost special devices. However, the research group at Surrey University has developed a mobile, low-cost and easily hidden device to read NFC payment cards using longer distances. They succeeded in reading data from a distance of 45-80cm [9]. Figure 16 shows the simple coil antenna used it this device.

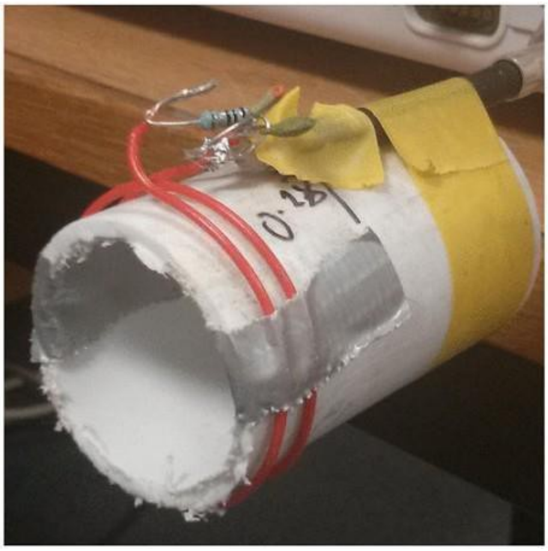


Figure 16. The coil antenna used by the research group at Surrey University [9].

CONCLUSION

The data security of the existing systems is insufficient. It does not mean that there isn't any system with sufficient security. Problems begin, when the manufacturers tend to produce low-cost products which are as simple as possible to implement into the old existing systems. It is possible to produce fully secure access control and contactless payment card applications using presented data security methods, but the cost of these systems is substantial.

As an example of a bad RFID security, there are alarm systems for sale, suited for private household use. The system is possible to turn on and off by using an RFID identifier. It is simple to copy this identifier to shut down the alarm system with or without permission and even by accessing the reader's electronics.

The data security level of contactless payment cards is also insufficient; in some ways even worse than in the case of older RFID systems. A large number of mobile phones include the NFC feature, which makes it possible to read and exploit payment cards. Additionally, reading does not require any special know-how or extra work, because the reader programs are free and legal to download in some online shops. The payment card owner may never notice the data theft, because it happens electrically; not physically. It is possible to produce secure contactless payment cards, but the cards today are utmost liable to malpractice.

In comparison, to read a specific RFID identifier you need a specialized device that has the same frequency, data coding and modulation format as the identifier but to read NFC contactless payment card all you need is a mobile phone with NFC capability and an application to display the data.

The Finnish data security company ***Nixu*** and many other sources have mentioned, that it is simple to read data from payment cards. Still every bank, which offers contactless payment cards, underline the good security level of cards.

There is no simple, fast and low-cost solution to data security problems. More powerful encryption and identification also require more powerful devices, which also cost more. In some cases it is possible to increase data security by using other standards than those used globally. The problem is that their implementation into older systems and world-wide standardization eases also the work of the misuse of the systems. It will most likely take many years before the systems begin to change and become more secure.

REFERENCES

[1] Arnall, T., ”RFID tags”, Yahoo! Inc, 2007, [Cited March 26, 2015], https://www.flickr.com/photos/timo/1616057288/in/photostream/

[2] BBC, “World’s tiniest RFID tag unveiled”, Brittish Broadcasting Corporation, 2007, [Cited March 26, 2015], http://news.bbc.co.uk/2/hi/technology/6389581.stm

[3] Bishop Fox, “Tastic RFID Thief”, Bishop Fox, 2013, [Cited March 31, 2015]. http://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/

[4] Bonsor, K. & Fenlon, W., “How RFID Works”, InfoSpace LLC, 2007, [Cited March 26, 2015], http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm

[5] Brown, F, “RFID Hacking: Live Free or RFID Hard”, Bishop Fox, 2013 [Cited March 31, 2015], http://www.bishopfox.com/download/837/

[6] Chandler, N, “What’s an NFC tag?”, InfoSpace LLC, 2012, [Cited March 26, 2015], http://electronics.howstuffworks.com/nfc-tag1.htm

[7] CNRFID, “RFID frequency spectrum”, French National RFID Center, [Cited March 24, 2015], http://www.centrenational-rfid.com/rfid-frequency-ranges-article-16-gb-ruid-202.html

[8] Dayal, G., “How they hacked it: The MiFare RFID crack explained”, Computerworld Inc, 2008 [Cited March 31, 2015]. http://www.computerworld.com/article/2537817/security0/how-they-hacked-it--the-mifare-rfid-crack-explained.html

[9] Diakos, T.,Briffa, J.,Brown, T. & Wesemeyer, S., “Eavesdropping near-field contactless payments: a quantitative analysis”, The Institution of Engineering and Technology. [Cited April 4, 2015]. http://digital-library.theiet.org/docserver/fulltext/10.1049/joe.2013.0087/JOE.2013.0087.pdf?expires=1427888678&id=id&accname=guest&checksum=10C50DAA7ABEC30E532C0E93B1F81A60Diacos

[10] EMVCo, “EMV Integrated Circuit Card Specifications for Payment Systems; Book 3: Application Specification”, EMVCo LLC, 2011 [Cited March 30, 2015], http://www.emvco.com/download_agreement.aspx?id=654

[11] EMVCo, “EMV Contactless Specifications for Payment Systems; Book A: Architecture and General Requirements”, EMVCo LLC, [Cited March 25, 2015], http://www.emvco.com/specifications.aspx?id=21

[12] EPCglobal, “EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID”, GS1 AISBL, 2013 [Cited March 30, 2015], http://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_2_0_0_standard_20131101.pdf

[13] Finkenzeller, K., “RFID Handbook. 2.p.,new. p.”, West Sussex: Wiley. 2003

[14] Franken, Z., “Physical Access Control Systems”, UBM Tech, 2008, [Cited March 30, 2015], https://www.blackhat.com/presentations/bh-dc-08/Franken/Presentation/bh-dc-08-franken.pdf

[15] Gaudi, S., “RFID hack could crack open 2 billion smart cards”, Computerworld Inc, 2008, [Cited March 31, 2015], http://www.computerworld.com/article/2537619/mobile-apps/rfid-hack-could-crack-open-2-billion-smart-cards.html

[16] HID Global, “FlexKey Keytag”, Galaxy Control Systems, 2006, [Cited March 30, 2015], http://www.galaxysys.com/data/docs/1407954514_hid-understanding_card_data_formats-wp-en.pdf

[17] HS. 2014, ”Jo sadoillatuhansilla suomalaisilla on lähimaksukortti” Helsingin Sanomat, December 26, 2014, [Cited March 31, 2015], http://www.hs.fi/talous/a1419560430271

[18] Impinj, ”RFID Standards”, Impinj Inc, [Cited March 25, 2015], http://www.impinj.com/resources/about-rfid/rfid-standards/

[19] IZT, Empa & BSI, “Security Aspects and Prospective Applications of RFID Systems”, Bundesamt für Sicherheit in der Informationstechnik, 2004, [Cited March 31, 2015], https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/RFID/RIKCHA_englisch_Layout_pdf.pdf;jsessionid=6E6A4D73F24D45713130FD7489255E24.2_cid359?__blob=publicationFile

[20] Kalmi, R.., ”Pankit tuputtavat uutta tekniikkaa – kuluttajia pelottaa”, Taloussanomat, June 5, 2013, [Cited March 31, 2015], http://www.taloussanomat.fi/raha/2013/06/05/pankit-tuputtavat-uutta-tekniikkaa-kuluttajia-pelottaa/20137977/139

[21] Lee, E., “NFC Hacking: The Easy Way”, Korben.info, 2012 [Cited March 31, 2015], http://korben.info/wp-content/uploads/defcon/SpeakerPresentations/Lee/DEFCON-20-Lee-NFC-Hacking.pdf

[22] Minto, R.., “Disabling contactless payment cards, or preventing ‘card clash’ with Oyster”, Robin Minto, 2014, [Cited March 26, 2015], http://robinminto.com/blog/post/2014/03/21/Disabling-contactless-payment-cards-or-preventing-card-clash-with-Oyster

[23] NFC Forum, “NFC Data Exchange Format (NDEF)”, NFC Forum, 2006, [Cited March 30, 2015], http://members.nfc-forum.org/specs/spec_license/document_form/custom_layout?1427738926323

[24] Nixu, ”Etäluettavien maksukorttien turvallisuudesta” Nixu Oyj, 2013, [Cited March 31, 2015], http://www.nixu.com/fi/blogi/2013-05/et%C3%A4luettavien-maksukorttien-turvallisuudesta

[25] Nordea, ”Lähimaksaminen”, Nordea Pankki Suomi Oyj, [Cited March 31, 2015], http://www.nordea.fi/Henkil%C3%B6asiakkaat/P%C3%A4ivitt%C3%A4iset+raha-asiat/Kortit/L%C3%A4himaksaminen/1607912.html?searchPhrase=l%u00e4hi&bb=0

[26] OP, ”Lähimaksu”, Osuuspankki, [Cited March 31, 2015], https://www.op.fi/op/henkiloasiakkaat/kortit/kortin-kaytto/lahimaksu?cid=151670031&srcpl=3

[27] Paget, C., “RFID for Beginners++”, UBM Tech, 2007, [Cited March 31, 2015], https://www.blackhat.com/presentations/bh-usa-07/Paget/Presentation/bh-usa-07-paget.pdf

[28] Poole, I., “NFC Near Field Communication Tutorial”, Adrio Communications Ltd, [Cited March 24, 2015], http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-tutorial.php

[29] Roberti, M., “The History of RFID Technology”, RFID JournalLLC, 2005, [Cited March 24, 2015], http://www.rfidjournal.com/articles/pdf?1338

[30] Schwartz, J., “Researchers See Privacy Pitfalls in No-Swipe Credit Cards”, The New York Times Company, October 23, 2006, [Cited March 31, 2015], http://www.nytimes.com/2006/10/23/business/23card.html?sq=RFID%20identity%20theft&st=cse&scp=2&pagewanted=all&_r=0

[31] Seppä, H., ”RFID-etätunnistus - mahdollisuudet ja uhat”, Eduskunnan tulevaisuusvaliokunta, Helsinki 2011, [Cited September, 2011], http://web.eduskunta.fi/dman/Document.phx?documentId=xh1821114514 5785&cmd=download

[32] Shepard S., “RFID Radio Frequency Identification”, McGraw-Hill, 2005

[33] Tait, D., “NFC-Enabled Cellphone Shipments to Soar Fourfold in Next Five Years”, IHS Inc, 2014, [Cited March 31, 2015] https://technology.ihs.com/490062/nfc-enabled-cellphone-shipments-to-soar-fourfold-in-next-five-years

[34] Violino, B. “RFID Business Applications”, RFID Journal LLC, 2005 [Cited March 24, 2015], http://www.rfidjournal.com/articles/pdf?1334

[35] Zetter, K. “Open Sesame: Access Control Hack Unlocks Doors”, Condé Nast, 2007 [Cited March 31, 2015], http://www.wired.com/2007/08/open-sesame-acc/