The Impact of Wireless Smart Cards on User Data Security

Alizée Perrin[1]

Cryptography Course, Faculty of Computer Science, University of Ljubljana

[1]ap6011@student.uni-lj.si

Abstract — **The essential aim of this report is to introduce the notion of wireless smart cards by describing the background of such technology, its operation and its association with the cryptography field.**

***Keywords*— Cryptography, Wireless, Smart Cards**

I. Introduction

The arrival of the Internet of Things and 4G wireless communications as well as machine-to-machine applications like Apple Pay are driving demand for smart card technology.

Smart cards are becoming more and more prevalent in fields such as personal identification and entitlement schemes at regional, national, and international levels. In 2016, nearly 9.8 billion devices using smart card technology shipped.

The contactless technology had a slow start, but today it is a new-wave revolution. It was the Seoul Bus Transport Association which launched the world's first-ever contactless payment card for bus and rail commuters in 1995 in the South Korean capital. Now known as the UPass, similar cards have been widely adopted in cities all around the world, and in other lines of business.

Through this report, we will try to identify the impact of wireless smart cards on security of data transit and on users privacy.

II. Description

A. General

A smart card is a device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or memory chip alone. This microcontroller gives smart cards the ability to store large amounts of data and to carry out their own on-card functions, such as encryption or mutual authentication.

Wireless (or contactless) smart cards are closely related to contact smart cards. But they also include a small antenna and communicate with a reader through a contactless radio frequency interface.

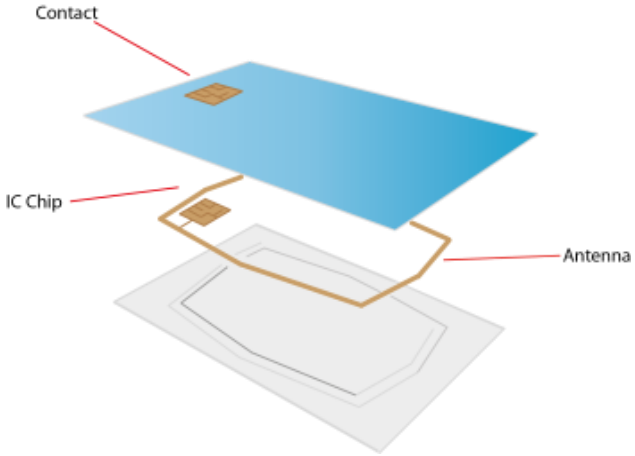

Figure. 1 Global concept of contactless smart card. Here is a dual interface : the card has both contact and contactless technologies.

It should not be confused with the RFID technology (Radio Frequency Identification). In certain cases, it can be used for applications similar to those of contactless smart cards, but RFID devices usually do not include writeable memory or microcontroller processing capability.

It is also different from NFC (Near Field Communication). NFC is a set of specifications published by the NFC forum, with the particularity of using the technology both ways round. So, integrated into a phone, NFC can be used to make the phone behave like a contactless card (called card emulation) or as a card reader.

Contactless cards do use NFC technology to send and receive data from a terminal using inductive coupling, and RFID for identification, but these are three separate technologies.

B. Components

IC chip : the key component of contactless smart cards is the embedded Integrated Circuit. It contains the applications and data that make a card functional. It is either a microprocessor with internal memory, or a memory chip with non-programmable logic. The role of IC is to store, transmit and process data.

Antenna : inside the card an antenna coil – made of copper or aluminium – is connected to the chip, eliminating the need for an internal power source.

The card's body is generally made of plastic and protect the IC chip.

UID : Unique Identification number that enables the reader to properly identify the card.

C. Deployment & Applications

We can detail several examples of application of contactless smart card technology.

It is mostly used for payment. Beyond the security changes it brings to "classical" card payment system, it also creates profits for the banks, because banks collect banking fees on each purchase, and the number of purchases with contactless cards has significantly increased.

Contactless cards are similarly deployed in personal identity verification, such as the PIV card. It is a United States smart card that contains the necessary data for the cardholder to be granted to Federal facilities and information systems and assure appropriate levels of security for all applicable Federal applications. The criteria for PIV cards was established by Federal Information Processing Standard (FIPS) 201, which specifies the interface and data elements of the PIV card, the technical acquisition and formatting requirements for biometric data on the card and acceptable cryptographic algorithms and key sizes.

Electronic passports also employ contactless cards. An ePassport is a paper-based passport that embeds a contactless smart card chip and an antenna. The ePassport inlay can be embedded into its cover, into the polycarbonate Data Page, or as middle page of the ePassport booklet. The mandatory data stored into the ePassport chip include document type, document number, surname, first names, date of birth, person's gender, issuing State or Organization, nationality, date of expiry and encoded face.

Even if its use has been growing in the access control and network security, and authentication markets, the first application of contactless technology was in public transportation. Passengers just hold their card within two inches of a reader to pay or securely authenticate a traveller's ticket of pass. More than 800 cities around the world have already deployed the technology. The key drivers for contactless cards in transport are speed, convenience, and flexibility. It also reduces transport costs versus cash of paper tickets, and it is more environmentally friendly.

III. FUNCTIONING

A. General

Contactless smart cards are ISO standardized. It operates at 13.56 MHz. The typical operating distance is from 5 to 15 centimeters. Data content can be from 256 bits to 4k bytes and more, and memory can be segmented for multi-application use.

Information is stored on a chip embedded within the card. The power supplied to the card as well as the data exchanged between the card and the reader are achieved using magnetic or electromagnetic fields to both power the card as well as to exchange data with the reader.

When the card is brought into the electromagnetic field of the reader, the card chip is powered on.

Then, a wireless communication protocol is initiated and established between the card and the reader for data transfer.

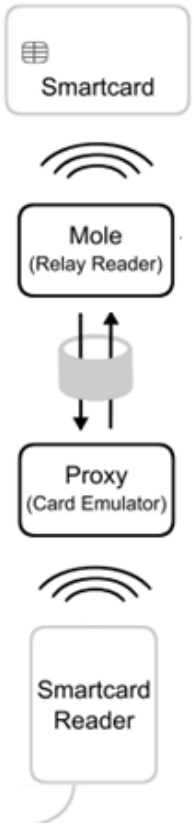

Figure. 2 Operation of the communication between a contactless card and a reader

The types of memory used in contactless cards are EEPROM, FRAM, and FLASH. The most widely used memory type for data storage in contactless cards is EEPROM : Electrically-Erasable Programmable Read-Only Memory. It allows to store informations that cannot be lost when the card is not powered.

But contactless microcontrollers also contain two other types of memory. Nonvolatile Read Only Memory (ROM) stores the card operating system and application code. Random Access Memory (RAM) is used for temporary storage of data during processing.

B. Communication protocols

The communication protocol used to structure data exchanged between contactless cards and readers is APDU (Application Protocol Data Unit), which is normalized and described is ISO 7816 part 4.

There are two categories of APDU : command APDU and response APDU.

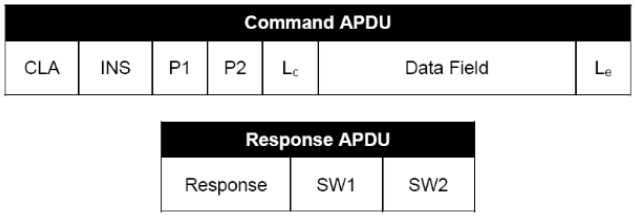

Figure. 3 Schema describing the composition of an APDU

The command is composed of a minimum of 4 bytes called HEADER, which has different fields :
-CLA : instruction class allows to identify the type of the command
-INS : the instruction code (read, write, authenticate…)
-P1 : first parameter of the command
-P2 : second parameter of the command
It can also have a BODY codifyed :
-L_c : number of bytes sent in DATA
-DATA : data sent
-L_e : number of bytes expected in the response

The response is composed of at least 2 bytes called TRAILER and codifyed :
-SW1 : codification of response type (normal, error, warning)
-SW2 : response detail
It can also have a BODY with DATA variable which corresponds to the data returned.

IV. Security and Weaknesses

A. *Security*

Three technologies can be implemented to protect data transit and some user informations (we will take payment cards as an example) :

-Chip technology, which improves the security of a payment transaction by providing a cryptographic card authentication that helps protects against the acceptance of counterfeit cards.

-Encryption, including end-to-end encryption (E2EE) or point-to-point encryption (P2PE) which can immediately encrypt card data at inception so that no one else can read it and use the card data for unauthorized transactions. With E2EE, the data is encrypted on the sender's system and only the recipient is able to decrypt it.
P2PE is a security solution that instantaneously converts confidential payment card data and information into indecipherable code at the time the card is communicating with the reader.

-Tokenization, which replaces card data with surrogate values that are unusable by outsiders and have no value outside of a specific merchant or acceptance channel

B. *Attacks & Weaknesses*

Various attacks are possible against smart card technology that can recover information from the chip.
Smart cards can be physically disassembled to gain access to the on-board microchip.

Hardware APDU sniffing devices also exist, even if recording the dialog between a card and a reader is not enough to clone the card. The private key used by the card to sign the transaction is never transmitted during the transaction and cannot be accessed, although differential power analysis can deduce the on-chip private key used by public key algorithms such as RSA while some implementations of symmetric ciphers can be vulnerable to timing attacks or differential power analysis as well.

In addition, the main physical weaknesses of wireless smart cards are water and steel. It can block radio waves.

V. Conclusion

We have stressed out the opportunities and the weaknesses of wireless smart cards. We have seen that this technology requires security parameters to be completely safe. If these parameters are not respected, the impact on user data privacy could be negative, because it could be stolen as easily as if it was cash.
We can say that this innovation still requires some adjustments.

However, it launched the contactless market and opened many opportunities. For the future of contactless smart card to be bright, it is important to look into several aspects and factors especially those resulted due to the rapid advancement in information and communication technology. Smart cards of the future may even stop resembling "cards" as smart card technology is embedded into rings, watches, badges, and other forms and factors that will make them remarkably convenient to use.

Bibliography

- Wikipedia community. Contactless smart card [Internet] Wikipedia. 2017 December 8; [cited 2018 January 11]. Available from: https://en.wikipedia.org/wiki/Contactless_smart_card
- Rouse M., Cobb M., Meckley J. Smart card [Internet] SearchSecurity. 2016 October 31; [cited 2018 January 11]. Available from: http://searchsecurity.techtarget.com/definition/smart-card
- Smart Card Alliance. Smart Card Technology FAQ [Internet] Smart Card Alliance. Unknown date; [cited 2018 January 11]. Available from: http://www.smartcardalliance.org/smart-cards-faq
- Smart Card Alliance. RFID Tags, Contactless Smart Card Technology and Electronic Passports : Frequently Asked Questions. Unknown date; [cited 2018 January 11]. Available from : https://www.securetechalliance.org/resources/pdf/RFID_and_Contactless_Smart_Cards_FAQ_FINAL_042105.pdf

- Jones R. Once it was touch and go, now contactless is a new-wave revolution [Internet] The Guardian. 2016 September 10; [cited 2018 January 11]. Available from : https://www.theguardian.com/money/2016/sep/10/contactless-cards-wave-pay-oyster-london-use
- Barclay Card. Hands off: a short history of contactless technology [Internet] Barclay Card. 2014 December 16; [cited 2018 January 11]. Available from : https://www.home.barclaycard/insights/contactless/contactless-timeline.html
- Wehr J., Adams J. Contactless chip manufacturers as a component of the card creation process [Internet] SecureIDNews. 2004 January 1; [cited 2018 January 11]. Available from : https://www.secureidnews.com/news-item/contactless-chip-manufacturers-as-a-component-of-the-card-creation-process-2/
- AVISIAN Staff. Tech 101: Contactless smart cards, A primer on radio frequency identification [Internet] SecureIDNews. 2011 December 13; [cited 2018 January 11]. Available from : https://www.secureidnews.com/news-item/tech-101-contactless-smart-cards/
- Wikipedia community. Electrically-erasable programmable read-only memory [Internet] Wikipedia. 2017 March 18; [cited 2018 January 11]. Available from : https://fr.wikipedia.org/wiki/Electrically-erasable_programmable_read-only_memory
- Gutmann P. Contactless Payment Systems: Credit Cards and NFC Phones [Internet] University of Auckland. Unknown Date; [cited 2018 January 11]. Available from : https://www.cs.auckland.ac.nz/~pgut001/pubs/contactless_payment.pdf
- Baker T. What is the difference between NFC and contactless ? [Internet] Quora. 2011 April 23; [cited 2018 January 11]. Available from : https://www.quora.com/What-is-the-difference-between-NFC-and-contactless
- Wikipedia community. Application Protocol Data Unit [Internet] Wikipedia. 2013 March 20; [cited 2018 January 11]. Available from : https://fr.wikipedia.org/wiki/Application_Protocol_Data_Unit
- Perinel F. Le format APDU pour communiquer en NFC [Internet] Red Froggy. 2016 February 15 ; [cited 2018 January 11]. Available from : https://www.redfroggy.fr/le-format-apdu-pour-communiquer-en-nfc/
- Buetler I. Smart Card APDU Analysis [Internet] Compass Security. 2008; [cited 2018 January 11]. Available from : http://www.blackhat.com/presentations/bh-usa-08/Buetler/FBH_US_08_Buetler_SmartCard_APDU_Analysis_V1_0_2.pdf
- Ngu M., Scott C. How secure are Contactless Payment Systems ? [Internet] RSA Conference 2015. 2015 April 20; [cited 2018 January 11]. Available from : https://www.rsaconference.com/writable/presentations/file_upload/ht-w01-how-secure-are-contact-less-payment-systems_final.pdf
- EMV. Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization [Internet] EMV Connection. 2014 October 1; [cited 2018 January 11]. Available from : http://www.emv-connection.com/technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/
- Rouse M. Personal identity verification (PIV) card [Internet] WhatIs. Unknown date; [cited 2018 January 11]. Available from : http://whatis.techtarget.com/definition/personal-identity-verification-PIV-card
- D'Albore A. What is an ePassport [Internet] Embedded Security News. 2017 February 7; [cited 2018 January 11]. Available from : http://embeddedsecuritynews.com/2017/02/what-is-an-epassport/
- Mohammed L., Ramli A. R., Prakash V., Daud M. Smart Card Technology : Past, Present, and Future [Internet] UPM Serdand Selangor, Malysia. Unknown date; [cited 2018 January 11]. Available from : http://www.ijcim.th.org/past_editions/2004V12N1/Fijcimvol12n1_article2.pdf