The 7th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 15th 2012

AN ANALYSIS UPON PRESENT CONTACTLESS SMART CARD TECHNOLOGIES

Cmd. Valeriu ANTON

Navy Forces

Abstract:

In few years, the new electronic identity services will be introduced to the public in Romania. The system is based on the smart card where the identification information is stored. The goal of such a project will be to get an electronic identification (EID)-card for everyone, so the security of the cards will be an essential object of inspection. This paper is about electronic identity and smart card technologies focusing their emerging security problems. The main part of the paper is the descriptions of different attacks against the cards.

Key words: *IC – Integrated Circuit*
EID – Electronic Identification
ATM – Automated Teller Machine
PIN – Personal Identification Number
PKI – Public Key Infrastructure
MSD – Magnetic Stripe Data
EMV– Europay, MasterCard and Visa

1.Introduction

Firstly, a contactless smart card is any pocket-sized card with embedded integrated circuits (IC) that can process and store data, and communicate with a terminal via radio waves. When the old magnetic stripe cards could be used only as a static identification tool for specific operations (bank cards) or as a very small magnetic memory (telephone cards), the IC in a smart card makes it possible to use the card for much complex operations.

Secondly, is also characterized as follows:

- Dimensions are normally credit card size: 85.60 × 53.98 × 0.76 mm;
- Contains a security system with tamper-resistant properties (e.g. a secure crypto processor, secure file system, human-readable features) and is capable of providing security services (e.g. confidentiality of information in the memory);
- Asset managed by way of a central administration system which interchanges information and configuration settings with the card through the security system;
- Card data is transferred via radio waves to the central administration system through card reading devices, such as ticket readers, ATMs etc.

2. Smart cards

2.1 Background

AN ANALYSIS UPON PRESENT CONTACTLESS SMART CARD TECHNOLOGIES

Smart cards are slowly replacing the old-fashion magnetic stripe cards. The old cards have very limited memory and their information security is very limited. Most of the people had considered the old cards safe before that but nowadays their weaknesses are better known. Copying the magnetic stripe card is not an expensive action. That can´t happen with IC cards because the card itself verifies the PIN code and the card can´t be copied, at least not so fast and cheap as the magnetic stripe card.. Because an IC card actually includes a working computer, the contents of the memory can more easily be hidden.

Since first deployed for the Octopus card scheme in Hong Kong in 1997, smart cards with contactless interfaces have been increasingly popular for payment and ticketing applications such as mass transit. Globally, contactless fare collection is being employed for efficiencies in public transit. In more recent times, Visa and MasterCard have agreed to standards for general "open loop" payments on their networks, with millions of cards deployed in the USA, UK, France and globally. Smart cards are being introduced in personal identification and entitlement schemes at regional, national, and international levels. Citizen cards, drivers' licenses, and patient card schemes are becoming more prevalent.

2.2 Specification

There are two forms of the IC card, contact and contactless. The contactless card may have an own power supply as it is with the "Super Smart Cards" which have an integrated keyboard and LCD display. The operational power can also be supplied to the contactless card with an inductive loop.

2.3 Readers

Contactless smart card readers use radio waves to communicate with, and both read and write data on a smart card. When used for electronic payment, they are commonly located near PIN pads, cash registers and other places of payment. When the readers are used for public transit they are commonly located on fare boxes, ticket machines, turnstiles, and station platforms as a standalone unit. When used for security, readers are usually located to the side of an entry door.

3. Applications

3.1 Transportation

Since the Octopus card in 1997, numerous cities have moved to the use of a contactless smart card as the fare media in an automated fare collection system. In a number of cases these cards carry an electronic wallet as well as fare products, and can be used for low-value payments.

3.2 Contactless bank cards

Starting around 2005, a major application of the technology has been contactless payment credit and debit cards. Some major examples include:

ExpressPay - American Express

PayPass - MasterCard

Zip - Discover

payWave - Visa

Roll-outs started in 2005 in USA, and in 2006 in some parts of Europe (England) and Asia (Singapore). In USA, contactless (non PIN) transactions cover a payment range of ~$5–$100.

In general there are two classes of contactless bank cards. Magnetic Stripe Data (MSD) and Contactless EMV (Europay, MasterCard and Visa**)**.

Contactless MSD cards are similar to magnetic stripe cards in terms of the data they share across the contactless interface. They are only distributed in the USA. Payment occurs in a similar fashion to mag-stripe, without a PIN and often in off-line mode (depending on parameters of the terminal). The security level of such a transaction is better than a mag-stripe card, as the chip cryptographically generates a code which can be verified by the card issuer's systems.

Contactless EMV cards have two interfaces (contact and contactless) and work as a normal EMV card via their contact interface. The contactless interface provides similar data to a contact EMV transaction, but usually a subset of the capabilities (e.g. usually issuers will not allow balances to be increased via the contactless interface, instead requiring the card to be inserted into a device which uses the contact interface). EMV cards may carry an "offline balance" stored in their chip, similar to the electronic wallet or "purse" that users of transit smart cards are used to.

3.3 Identification

A quickly growing application is in digital identification cards. In this application, the cards are used for authentication of identity. The most common example is in conjunction with a PKI (Public Key Infrastructure). The smart card will store an encrypted digital certificate issued from the PKI along with any other relevant or needed information about the card holder. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and the use of various smart cards by many governments as identification cards for their citizens.

When combined with biometrics, smart cards can provide two or three factor authentication. Smart cards are not always a privacy-enhancing technology, for the subject carries possibly incriminating information about him all the time. By employing contactless smart cards, that can be read without having to remove the card from the wallet or even the garment it is in, one can add even more authentication value to the human carrier of the cards.

3.4 Other

The Malaysian government uses smart card technology in the identity cards carried by all Malaysian citizens and resident non-citizens. The personal information inside the smart card (called MyKad) can be read using special APDU (Application Protocol Data Unit) commands.

4. Common attacks on smart cards

4.1 Introduction for the attack classification

The smart card marketing people often claim that smart cards cannot be attacked successfully. But, nowadays, this is definitely not the case.

One method for classifying the possible attacks against smart cards is to categorize the attacks by the parties involved in the attack action [1]. The different parties in the smart card based system are the following:

The **cardholder** is the person who uses the card.

The **data owner** is the party who has the control of the data in the card. As in case of the electronic ID card, the data owner is the person whose secret key is contained in the card.

The **terminal** is the device, which offers the interaction between the card and the outside world. As with EID card, this is the card reader and the computer attached to the reader with the screen and the keyboard.

The **card issuer** is the party who has issued the smart card. This party controls the operating system and the data in the card.

The **card manufacturer** is the party who produces the card itself.

The **software manufacturer** is the party that produces the software for the card.

The attack types described in the next sections are the ones that can be considered with EID cards. Attackers are considered as two different classes: those who are parties to the system and those who are outsiders.

4.2 Classifying the attackers

The possible attackers can be divided to following categories: [2]

Class I (clever outsiders). This type of attackers are often intelligent but their knowledge of the system may be insufficient. They may have access to only moderately sophisticated equipment. They seldom create weakness of the system by themselves but try to take advantage of an existing weakness.

Class II (knowledgeable insiders). They have some specialized technical education and experience. The may understand some parts of the system and have a potential access to most of it. They often have high quality tools and instruments for analysis.

Class III (funded organizations). They may assembly teams of skilled specialists and they also have great funding resources. They are able to perform some in-depth analysis of the system, design powerful attacks and use the most advanced analysis tools.

4.3 Attacks by the terminal against the cardholder or data owner

This attack class is also known as the *trusted terminal problem*. The cardholder must somehow trust to the terminal that the terminal does what the cardholder wants and only that. This is very important in EID system because of the digital signing service. If the cardholder wants to sign some data, he/she must have some confidence that the terminal doesn´t sign anything else than just the wanted data. The above scam with the old magnetic stripe cards is the attack of this type. The terminal copied the card so that the cardholder didn´t notice anything.

4.4 Attacks by the cardholder against the terminal

This type of attack is performed with fake or modified cards running some rogue software. The goal is to break the protocol between the card and the terminal.

4.5 Attacks by the cardholder against the data owner

With EID cards, this type of attacks are relevant only if the card has been stolen. The data owner should be the only one who knows the PIN code for the data (secret key) so the new cardholder tries to get or modify the data some other way. These following

techniques have already used with great success against some pay-TV- and public telephone cards [2]. Also some early smart cards have been successfully hacked.

Tamper resistance must be considered more careful in smart card systems than in the old magnetic stripe card systems. The old systems had cryptographic systems in a secure place and the passcodes for the card were verified remotely from the card terminals. In smart card system, the card itself must be secured very carefully because the cryptographic keys are in the card itself and not in some safe deposit of the bank. The attacker can steal a card and take it to the private lab and examine it with care and time. When planning the tamperproofing, it´s important to know the class of attackers we want the cards to be protected against.

The card may be vulnerable to the attacks, which try to operate the card in an environment, which is against the specifications of the card. For example, the card can be driven with unusual clock rate or voltage levels and this can cause some malfunctioning in the poorly secured card. This failure can cause an operating system crash or some output of secure data. These techniques are called **differential fault analysis** .

The attacker may also try a straight physical attack to the card like removing secure components or burning some parts of memory. The IC may not be so difficult to remove from the card than one might expect. The circuit in some of the cards can be successfully removed with some quite cheap home lab equipment so this type of attack could be performed even by class I attacker [2]. There is also some very sophisticated attack methods so tamperproofing is very essential process for smart card manufacturers.

Differential power analysis is quite new attack type, which has successfully used against certain smart cards . The power consumption of the card is measured and analyzed. If an attacker has some hint what the card might be doing when measuring the power consumption, the attacker can obtain a quite accurate picture of the internal behavior of the card. Multiplication, division and other arithmetic operations consume different amounts of power.

4.6 Attacks by the issuer against the cardholder

These types of attacks are typically some violations against the privacy of the cardholder. This is very important in the EID system because the issuer is able to generate the secret keys for the cardholder.

4.7 Attacks by the manufacturer against the data owner

When the data owner uses the card, how can he/she be sure what programs there are really running in the card?

For example, when verifying a pin code fails, how can we ensure that the card has actually tried to verify it?

Or what if the card accepts all the pin codes?

There are many possibilities for the manufacturer to attack against the data owner and these attacks would obviously be very harmful.

5. Security problems in smart card based EID system

5.1 General securing issues

When planning the tamper proofing the card and other security issues it´s important to classify the possible attackers against our system. EID system must obviously be protected against class II and even the class III attackers whereas for example in a case of PayTV-cards it could be enough if we just secure them against class I attackers.

Terminal and card reader security can be improved by setting some limitations for the allowed transactions and other user actions. For example, we could allow the user to sign only certain types of data. Also some time limits like actions per minute or maximum time for the terminal to access the card can be set. When the users will have their own card readers and software at home, it´s very difficult to be sure that everybody has trusted security modules. Because of that, the most secure attack prevention mechanisms are those which have nothing to do with the interface between the card and the terminal. They monitor the terminals operations and log all the suspicious behavior in the information net.

The manufacturer of the card must be trusted organization, which has well known products. Also the organization, which has the responsibility for initializing the keys the card, must be known to be very reliable. The system, which creates the key pair, must secure itself that the secret key cannot be revealed. The organization, which personalizes the cards, must have a very high-class quality assurance. It must also have a clear way to administer the other important information for activating the card. The register organization must also be reliable and it must have a secure way to identify a person when issuing and registering his/her EID card.

The users themselves must understand their own responsibilities in the EID system and they must also have enough skill to use it. The authority, which offers some EID-related services, must ensure that the services work the way they are supposed to and that the secure information is certified and it can not be changed when delivered. The same authority must also be able to put time stamps for the data it handles. Also the help desk and blocking list services must be secure and some limited number of staff must be authorized to administer them and identify the users.

6. Conclusions

Electronic identification will come as a part of every-day life of all citizens. With that card, several public services can be reached from the Internet and other remote terminals. Internet is not safe by default so we must use strong public-key cryptography and other methods to improve the network security.

We specified smart card as a plastic card, which has an integrated circuit included. Attacks against smart cards can be classified by categorizing them by the parties involved in the attack action. Attackers can be categorized based on their skills and available funding resources and tools. EID Smart card system must be secured against the most powerful attackers. We must tamperproof the cards and also secure the card readers and computers, which they attac

References:

[1] http://www.globalservices.bt.com/uk/en/solutions/monitor_my_network_security
[2] http://www.cl.cam.ac.uk/~rja14/tamper.html
[3] http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/smartcard/smartcard.html
[4] http://en.wikipedia.org/wiki/Contactless_smart_card