SMART CARD (IN-)SECURITY

Philip KEERSEBILCK[1], Wim VANHOUCKE[2]
KAHO St Lieven
Associated partner of University of Leuven
Department of Electrical Engineering
Gebr. Desmetstr. 1, B9000 Ghent, Belgium
[1]Philip.Keersebilck@kahosl.be
[2]Wim.Vanhoucke@kahosl.be

Abstract. *In the last years, a lot of organisations have turned to smart cards lately. Today's applications require more and more security and functionality than before. Smart cards, equipped with a microprocessor and a great number of security features, can enhance information security. Yet media still reports regularly on fraud and attacks on smart cards. This paper evaluates smart card systems and gives a technical overview of the threats in crypto devices such as smart cards. It discusses the security of the smart card in a number of aspects and domains. There are in general two approaches for attacks on smart cards: invasive or internal attacks, where the chip will be opened, and non-invasive or external attacks, where the card will remain intact. To counter these types of attacks, chip manufacturers as well as card operating system developers, have developed countermeasures to provide protection against these various attacks.*

Keywords: *smart card, information security, hacking, computer security.*

1. Introduction

Since the tragedy of 11 September, a lot of organisations are turning to systems with high(er) security level. The aim is clear: make information readily available to those who need it, while at the same time protecting the privacy of individuals and keeping their information safe.

Today, over one billion smart cards are used in banking systems, telecommunication, healthcare and transportation. Actually, military organisations use more and more smart cards for electronic identification and access control.

The smart card seems to be a superior tool for enhancing system security and provides a place for secure storage. One of the features provided by most of the smart card operating systems, is the cryptographic facilities. They provide encryption and decryption of card data; some of them can even be used to generate cryptographic keys. The secret of the cryptographic algorithm, the keys stored and the access control inside the smart card become the targets of the attackers.

Nowadays some companies and cryptographers claim to be able to break the smart card and its controller. Some of them perform logical non-invasive attacks, others attack the card physically. As always, stories are incomplete and here I will try to give a more balanced view of the real picture. This paper presents a technical overview of the security features and the threats in smart card security.

2. Smart card as secure platform

A smart card can be considered as a self-contained, micro-processing unit, and this self-containment makes a smart card more resistant to casual attack [1]. A smart card does not need to depend upon potentially vulnerable external resources, and this characteristic, plus the portability of the card itself, makes the smart card a useful technology in applications that require strong security protection and authentication.

The three main features of the smart card, which provide its secure nature are respectively:

1. The physical structure of a smart card

Current ISO Standards (7810, 7816) [2][3] make the smart card physically stable. The size, thickness and bend requirements for the smart card are designed to improve the card security.

The serial interface speed between the card and a card acceptance device is limited (ISO 7816) to 9600 bits per second. This is enforced to limit the time efficiency of a brute force attack on the card. The security of the chip starts with the design of the chip itself, which is carried out on secure CAD-systems in facilities with tight access control. The card also passes through several clearly defined stages, in order to prevent counterfeit. During manufacturing and testing, links are used to provide access to testing functions or to load serial numbers into the card; keys are blown after use. When the chip is first created, a fabrication key is created to prevent the chip from modification before it can be disassembled into the plastic house. The key is unique to every chip, and is derived from a master key owned by the chip manufacturer. Once the key has been tested, the fabrication lock is blown before the chip is passed to the smart card manufacturer. The card manufacturer embeds the chip in the card, and replaces the fabrication key with a personalization key. The personalization is complete by blowing the relevant lock, so all of the data entered can never again be altered.

Subsequently, the card is passed to the card distributors. When the card is issued to a user, all necessary data files and application(s) are written into the chip. This includes personal information of the card holder, a PIN (personal identification number) and a utilization lock which indicates that the card is authorized to be used. The PIN may be optionally replaced by a biological identifier, e.g. a fingerprint, an iris scan, …

Card issuers use methods to prevent forms of postal interception. Two common methods are to create a time gap between the card being issued and the beginning of its validity (during which time the issuer checks that the card has been received) or to require a separate action that includes an identity control (e.g. by an on-line terminal) to activate the card.

2. Memory structure

The memory of a smart card chip is controlled by memory-management circuits, which provide hardware protection against unauthorised access. This protection uses a hierarchy of files (directory system), similar to other common operating systems, but the file structure contains additional accessing conditions and file status fields in the file headers [4]. ISO 7816-4 defines the security mechanisms to provide both authentication and confidentiality of the data and keys.

A “file lock” attribute is used to prevent a file from being accessed [5]. Files on the smart card can have different levels of access control, and PINs on the card can facilitate smart card file access. The “always” condition allows access without restriction. Pin management, present in the smart card operating system, can lock the smart card in the case of invalid pins, being presented to the CAD. Indeed, there are usually two different cardholder verification PINs that allow access to different files or functions. One pin is the primary cardholder identifier. The second PIN is used to “unblock” the card if the user has failed to provide the first PIN correctly with a certain number of trials. The “never” condition forbids access to files.

3. Transaction procedure

All chip cards make use of a single bidirectional serial I/O-interface. The electrical connection is implemented through contacts or by electromagnetic coupling and is defined by ISO 7816-3. Given the on-board computing power of the smart card, it is possible to achieve off-line transactions and verifications between the smart card, CAD and other devices. Moreover, the chip manufacturer encrypts data and codes stored on the card, which makes the circuit chip tough to be forged.

The smart card is only useful when used in conjunction with a CAD (card acceptance device). The smart card and the CAD use a mutual active authentication protocol to accurately identify each other. Wireless smart cards work in a similar way as RFID tags, and are likely to be more popular because they are thicker and easier to use than a device in which the card is inserted. This eliminates the need for the user to interact directly with any device other than their card. This means, however, that the cards are vulnerable to attacks while they are in user’s pocket, without the user’s knowledge!

In some applications (e.g. financial transactions) and due to security reasons, cards must be physically inserted into a CAD. Other applications (e.g. identity control) use sometimes cards with a biometric feature (e.g. fingerprint, iris scan, …)

3. Smart card security threats

Smart cards are very popular targets for attackers, for diverse reasons:

- Smart cards are portable: the attacker can easily carry them to a hacker environment.
- Smart cards are cheap and easy to acquire.
- The opportunities of financial gain.

Manufacturers are well aware of these temptations and invest great amounts of money to improve the security of their products. In practice 100 % security is never possible and designers *and* attackers of such systems are continuously challenging each other.
There are in general two types of attacks:

- Invasive tampering attacks, where the chip will be opened.
- Non-invasive attacks, where the card will remain in the plastic holder.

The overall security of a system is established by the synergy between physical (hardware), logical (software) and organisational security measures (e.g. key management). Therefore, the preferred approach for a security evaluation is to make an internal attack analysis and an external attack analysis.

4. Invasive attacks

Principle

This section discusses attacks in which chip *hardware* is analysed and/or modified. These attacks, which involve performing operations directly on the chip, can be designed only by trained professionals who have access to expensive equipment. For this reason, most attacks are in fact designed in research laboratories and in evaluation laboratories. In general, invasive attacks can be considered as quite powerful but often destructive. Therefore, hackers buy several specimens of a chip card.

Tampering techniques

In the production process of a smart card, the chip is glued to the metal contacts, and thin gold wires are used to implement the electrical connections. Further, the chip is covered with a layer of epoxy resin and finally pasted into a plastic card. But vice versa, the chip can quite easily be removed from the card This can be realised by using a sharp knife; now, the epoxy becomes visible. It can be dissolved by using some (drops of) nitric acid. Nitric acid does not attack the silicon of the chip nor the content of EEPROM [6].
After depackaging, the next step is to analyse the chip. Optical microscopes with a CCD camera and/or scanning electron microscopes (SEM) are used to identify basic structures such as bus (address and data) lines and other functional modules. By reverse engineering, the attacker studies connectivity patterns and tries to reconstruct the layout in order to access memory values.
A popular tool for invasive attacks is the use of *micro-probe stations*. Microprobes are very small probes, making part of an optical microscope. On the arm of such a special microscope, the attacker installs an extremely small probe which allows him to establish electrical contact with the chip. The advantage of this technique is that signals of bus lines can be measured, without damaging them. In this way, probes can monitor all data exchanges (e.g. key information) between the processor and the memories.
And vice versa, it is also possible to force signals on the circuitry, so the processor will e.g. execute disturbed operations. In combination with an amplifier and digital signal processor, it is possible to reveal running program code and keys. In some cases (e.g. multi-layer chips), connections are too small to view with probe stations; they can then be "enlarged" by a FIB *(*Focused Ion Beam). A FIB consists of a vacuum chamber with a particle gun and beam, which uses ions instead of electrons [7]. By

adding different gasses to the ion beam, chip material can be changed or even removed, e.g. blown fuses of certain circuits can be reconnected.

Protection against invasive attacks

In the past years, chip manufacturers use very high technology to attain physical security and limits the success of invasive attacks. An overview:

-*Multi-layered chips*: realise not only a high density of semiconductors on the surface, but even spreading of functions across several layers, in a seemingly random fashion. Elements regarded as vulnerable to analyse (e.g. ROM) will be buried as far as possible in a lower layer.
-*Sensors*: detect ion of nitric acid or even light, temperature.
-*Chip size*: the size of internal components on a chip surface is strongly reduced : from about 0,5 µm to less than 150 nm!
-M*etallization* layers, which protect the chip against atmospheric effects and must usually be removed for any intrusive analysis.
-*Glue Logic*: alternating sorts of resin are added to the chip, so different sorts of solvents must be used to solve these resins. Preferably, soluble components are used so that the chip is useless after the operation.

5. Non-invasive attacks

Principle

Non-invasive attacks try to analyse or change the behaviour of the smart card. This kind of attacks does not harm the smart card and are not card-specific. The attacker observes the card during calculations, while having the possibility to manipulate the card reader. The equipment used in this kind of attacks can be considered as simple. In contradiction with invasive attacks, the designer of non-invasive attacks must have profound knowledge of both hardware and software.
Smart card processors are often victim of non-invasive attacks, because their hardware is quite sensitive to variations in their environment such as power consumption, electromagnetic radiation, time, voltage, temperature, clock frequency, ... Attacks using these phenomena try to analyse or manipulate the behaviour of the chip [6]. The following attacks are discussed: timing attacks, power consumption attacks, induced errors and (in brief) logical attacks.

Attack classes and countermeasures

1. Timing attack on RSA.

The key in the card determines not only the output of a calculation, but the duration as well. In a timing attack, the attacker manages the card reader and is able to measure the time gap between the start and the end of the execution of the key operations. This information can lead to information about the secret keys, especially in vulnerable systems. E.g. by carefully measuring the amount of time required to perform private key operations, an attacker might find fixed Diffie-Helman exponents, factor RSA keys, and break other cryptosystems. If a unit is vulnerable, the attack is computationally simple, and requires only known cipher text [7].
A usual *protection against timing attacks* is to execute superfluous calculations; this protection is executed on the level of sofwarecoding [8]. Naturally, the card operates slower due to the executions of these superfluous steps.

2. Power consumption attacks

A smart card does not possess a battery; it receives power from the card reader. The power consumption of a smart card can be monitored in an easy way. Inserting a measure resistor in the power line, the voltage of the resistor can be viewed in time by using an oscilloscope.
The power consumption is statistically correlated to the operations that are performed. Indeed, during the execution of an algorithm, the power consumption is strongly dependent of the used data, so parts of an algorithm can eventually be reconstructed. E.g. in DES,

moments of key rotations can easily be recognized in the power trace.

If information is retrieved from one run or several runs of power attack, we speak in terms of *single power attack* or *differential power attack*. In a single power attack, an attacker observes *visually* the power consumption of a system. Large features such as DES rounds, RSA operations, etc. may be identified.

Differential power analysis [9] can retrieve the key of a cryptographic algorithm by analysing several runs and comparing the mutual differences. The attacker needs to know either the input or the output (encrypted text) of the algorithm. Differential power analysis uses statistical analysis and error correction techniques to extract information about keys. This last technique is very powerful and became very popular in the last years.

Possible *protection against power attacks* are masking power consumption with digital noise or throwing random calculation into the mix. Another potential solution is randomizing the order of card computations so that in the end, the same computation is performed using different patterns of primitives. All of these potential solutions are ways to mask the giveaway patterns in the power consumption of the card. Other hardware techniques, used by the smart card industry, are reducing electromagnetic emissions, by use of a metal shield. On the level of application countermeasures, retry-counters are used to limit the number of trials of the attacker, e.g. the PIN-verification mechanism that blocks after three failures.

3.Deliberately induced errors

During its calculation time, the smart card is very depending on its existing environment. The active part is very small and disappears complete in the card reader. Research has been made about disturbing electronic circuits in the chip by realising an extreme environment.

The attacker introduces errors in plenty of ways [8]. In a *glitch* (or rapid transient) attack, the attacker generates a malfunction that causes one or more flip-flops to adopt the wrong state. The aim is usually to replace a single critical machine instruction with an almost arbitrary one. As result of this, the card generates an incorrect output, and in some cases, secret information can be revealed.

The most successful attacks use fluctuations in voltage supply. Sudden changes or interrupts in voltage, cause an incomplete execution of some instructions. In a power glitch attach, a short and well-tuned power glitch (e.g. a short interrupt of the power supply) may introduce a computational fault while the processor continues to execute the running program code.

Other techniques are based on exposing the card, during its operation time, to very extreme temperatures, or electromagnetic radiation (Rontgen or UV) or even mechanical forces.

If the card needs an external clock signal, it can be manipulated (clock-signal glitch), so switching errors occur in complex instructions. Because of this reason, most cards have actually an internal clock [10].

There are various protection methods against deliberately induced errors [11]. To counter *glitch attacks*, smart cards can be equipped with sensors to measure voltage, clock frequency, and temperature; mechanical tension in the chip can be detected by means of layers of a piëzo-cristal. In this way, each disturbed behaviour can be interpreted as an attack and blocks the card. Unfortunately, it is not possible to detect all induced signals.

Concerning countermeasures on the level of software, computing results twice and comparing both results is a rigid way to check the validity of the results.

4. Logical attacks

These kind of attacks make use of the external logical functions of the cryptographic device and look for specific software or protocol bugs that can be exploited [12]. These occur when a smart card is operating under normal physical conditions, while sensitive information is gained by examining the bytes going in and out the smart card. Logical attacks are not further discussed here, since they belong not to the scope of this paper.

Conclusions

Today's smart card chips, have been designed to offer a high resistance to various forms of attack using a combination of hardware and software defensive features.

Smart cards are tamper resistant but not tamper proof. Having different kind of attacks does not mean that smart cards are insecure. It is important to realise that attacks against any secure systems are nothing new or unique. Any systems or technologies claiming 100% security are irresponsible.

It is believed that smart cards offer more security and confidentiality than the other kinds of information or transaction storage. Moreover, applications applied with smart card technologies can be considered as one of the best solutions to provide and enhance their system with security and integrity.

A last point to consider is that security is a never-ending battle. As technology improves, both sides of the battle have better tools to work with. Smart card manufacturers invest each year millions of euros on improving security of smart card systems. So, the smart card is an important element of solution to security problems in the modern world.

References

[1] Chan Siu-Cheung Charles (2004), *An overview to smart card security*

[2] U.S. General service administration (2005), *Smart card standards and interoperability*, http://smart.gov/

[3] *Alt.technology.smartcards faq* (2005), http://www.faqs.org/faqs/technology/smartcards/faq/

[4] Keersebilck Ph. (2003), *Smart card technology based on Java*, white paper

[5] Rankl W. (2000), *Smart Card Handbook*, Wiley & Sons

[6] NIST (2004), *Card technology developments and gap analysis interagency report*, http://csrc.nist.gov/publications/nistir/nistir-7056.pdf

[7] Hagai Bar-El (2003), *Known attacks against smartcards*, http://www.infosecwriters.com/text_resources/pdf/Known_Attacks_Against_Smartcards.pdf

[8] Witteman M. (2002), *Advances in smartcard security*, http://www.riscure.com/articles/ISB0707MW.pdf

[9] Cryptography Research (2005), *A differential power analysis*, http://www.cryptography.com/resources/whitepapers/DPA.html

[10] Yahya Haghiri, Tarantino Thomas (2002), *Smart Card Manufacturing: a practical guide, Wiley,*

[11] Gemplus (2003), *Physical security of smart cards: test procedure proposal*, http://www.incits.org/tc_home/b105htm/b105Doc2003/N03-143-Sec-v.01.pdf

[12] Gary Mc Graw & Edward Felten (1999), *Java security – Hostile applets, holes and antidotes*,