**BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)**
**ISSN (P): 2348-0513, ISSN (E): 2454-471X,**
**Vol. 4, Issue 7, Jul 2016, 11-18**
**© BEST Journals**

# AN ANALYSIS OF SECURITY MECHANISMS IN SMART CARDS

**NAMAN KHULLAR**

R&D Department, Syscom Corporation Ltd**,** Uttar Pradesh, India

## ABSTRACT

Smart Cards are often endorsed to be one of the most secure portable storage devices. This technology can provide identification, authentication, data storage and application processing. This paper presents an overview of the Smartcard Security and the threats, which it faces like Logical, Physical and Side channel. The dangers caused by these threats are discussed along with its basic countermeasures.

**KEYWORDS:** Smart Card Security, Side Channel Threats, Logical Threats, Physical Threats

## INTRODUCTION

In today's world, we cannot imagine our life without Smart Cards. Be it a Credit card, ID card or a simple Metro card, Smart card has become an integral part of our lives. Smart card has evolved from a very simple phone cards to business cards made with inferior equipment into a complex technology security solutions that can now support a large number of applications.

Earlier generation smart cards use was limited to a memory chip that can hold a stored value, which is described as write once only. These were disposable and used as stored value cards for payphones. Today's applications or "Applets" require more support from the Operating System of the smart card. Yes, the smart card too has an OS; in fact it is just like a mini computer equipped with an OS, RAM, ROM and an EEPROM. Smart cards are now equipped with microprocessors and a significant number of security measures.

In addition, the smart cards also embed a cryptographic coprocessor. Because the common asymmetric cryptographic algorithms of the day (such as RSA) require very large integer math calculations, an□8 bit microprocessor with very little RAM can take on the order of several minutes to perform a□1024 bit private key operation. However, if a cryptographic coprocessor is added to the architecture, the time required for this same operation is reduced to around a few hundred microseconds. The addition of a cryptographic coprocessor can increase the cost of today's smartcards by 50% to 100%. But the cost is not the point of discussion as it adds on to the capabilities of the smart card. The smart card can now support popular security applications and protocols. It can be used to store highly confidential data, crypto keys and much more. This becomes a critical factor for operations such as digital signatures, authentication and non-repudiation. Eventually, though, the need for a cryptographic coprocessor and its associated cost will likely go away.

This paper gives an overview of the threats that prevail in the smart card industry. In addition we will also discuss about the counter measures that are taken to make the smart cards as secure as possible.

## ATTACKS TO SMART CARDS

There is no security system, which is unbreakable, or at least no one has designed such a system until now.

Designing secure systems is a matter of balancing costs and benefits, which means it is truly a matter of engineering. Availability, Integrity, and Confidentiality, can be only “partially” granted, and time and resources devoted to these requirements must be correctly balanced against other functional requirements.

Since the popularity of Smartcard has emerged, they become popular targets for attackers. Smartcard security threats are classified as follows:

- Logical Attacks: exploits that use bugs in the software implementation.□
- Physical Attacks: exploits that use analysis or modification of the smartcard hardware.□
- Side Channel Attacks: exploits that use physical phenomena to analyze or modify the smartcard behavior.

## LOGICAL ATTACKS

Smartcards have a single communication channel to exchange data with a smartcard reader. This channel is a serial interface where commands can be issued that the smartcard has to perform. The exchange of commands is in the form of a black box where only APDU’s are exchanged. Although smartcards are small computers, there are a number of command options that are available. Due to this complexity and time-to-market constraints it happens that hidden flaws that do not affect the normal behavior remain undetected during security tests. Logical attacks abuse these flaws to trick the smartcard into surrendering confidential data or allowing undesired data modifications.

- Hidden Commands: Smartcard operating systems can technically distinguish between more than 50,000 commands. Although practical use may require only a few commands, there may be some remaining and active commands from the initialization phase or from a previous running application. These commands may be abused to retrieve or modify the data in the smartcard.
- Parameter Poisoning and Buffer Overflow: Commands are accompanied by a number of different parameters that specify the exact request. An invalid parameter value or length may not be rejected, but misinterpreted and lead to surprising results. A simple, but sometimes effective, example is a file read command where offset and requested length exceeds the actual file size.
- File Access□: Smartcard file systems have detailed permissions on files and directories. For each and every file, there is a mechanism to define different access conditions. It may happen that the access permissions implemented allow more access than needed for specific files, thus creating a security hole. Complex interactions can occur when several distinct applications need to be accessed during one session, and operating systems may confuse access permissions.
- Malicious Applets: Smartcards that support multiple applications need to ensure application separation. The operating system should create a virtual environment where applets cannot harm or ever interact each other directly. If some how an attacker manages to download a rogue applet, or abuse a flaw in one applet, he may be able to compromise another security sensitive applet.
- Communication Protocol: Information exchange between smartcard and terminal is managed by a communication protocol that handles data flow control and error recovery. By sending messages outside the scope of the current state it may be possible to trick the smartcard into revealing secrets. Smartcards use a small message buffer within

the RAM memory to store operation results. They also keep a length field that indicates the length of the available buffer data. Whenever a message is not correctly received the terminal can request retransmission of the message. If a smartcard reader were to ask for retransmission of a message that had not yet been sent at all, a sloppy smartcard implementation may decide to send the buffer anyway. If at the same time the length field is not properly initialized the implementation may send a large part of, or even the entire remaining memory. Such a memory dump results in a complete surrender of all confidential data and secrets.

- Crypto-Protocol, Design and Implementation: Cryptographic protocols handle consecutive cryptographic operations to perform transactions. Cryptographic protocols must be carefully designed to avoid fallbacks with transactions. Some cryptographic schemes have fallback methods to enhance reliability in case of technical problems. These fallback methods may be less secure and attacks may benefit from creating fictitious mal-functions. Furthermore, many cryptographic algorithms are still proprietary and have never been publicly reviewed. They may be flawed and eventually be broken when the design leaks out. Finally, number generators may not generate enough randomness, thus becoming predictable.

## COUNTERMEASURES FOR LOGICAL ATTACKS

Logical attacks are dependent with the smartcard software complexity. Software developers know that the number of bugs grows with the size of the code. Some strategies to combat software bugs (including security flaws) are:

The sensitivity to logical attacks is dependent on the complexity of the software. Software developers are aware that the number of bugs increases with the increase in the size of the code. Some strategies to combat software bugs (including security flaws) are:

- Structured Design: create software in small functional building blocks that can easily be understood and validated.
- Formal Verification: use mathematical models to prove the soundness of functions.
- Testing: perform functional as well as complete experimental validation of the implementation.

In the field of smartcards there are a couple of methods that can be categorized like:

- Standardization of Interfaces and Applications: Reuse of older tested software decreases the chance of flaws.
- Convergence to the Java Card Operating System: An object-oriented language that was designed for security is conceptually more secure than the older monolithic operating systems without application separation [2]. The Java card OS does not allow the applications to interact with each other directly.
- Popularity of Evaluation Labs: a growing number of card manufacturers and card issuers use evaluation labs to get a certificate for their products. Despite these trends smartcards are far from immune to logical attacks. The growing software complexity will always bring in the risk of introducing new flaws. Careful design and validation may reduce the number and increase the difficulty of exploiting the flaws, though. Unskilled attackers may then no longer be able to find exploits. Still it cannot be guaranteed that the number of attacks will go down significantly.

## PHYSICAL ATTACKS

A smartcard chip may appear to be an electronic safe, but it is actually not all that secure. Although all its functions are encapsulated in one chip but it is possible to reverse engineer them. Physical attack methods require high-end lab equipment, but do provide powerful tools to perpetrate successful exploits.

These attacks can be performed by a numerous methods and tools. Some of them are described below:

- Chemical Solvents, Etching and Staining Materials: Etching materials are able to de-capsulate and accurately de-layer smartcards. The chip surface reveals the various building blocks in the chip. After this process the chip is accessible for optical or electrical analysis. The epoxy that fixates the chip into the card can easily be dissolved, but the removal of metal and silicon layers requires quite aggressive and dangerous chemicals that should only be handled by experts in a chemistry lab. Because modern chips contain multiple layers this is an essential step in reverse engineering. Staining is an advanced etching technique that uses differences in etching speed to reveal subtle material differences that define the ones and zeroes in some ROM memories. Many times during these processes the smart card is harmed and is made useless and sometimes responses even thought arbitrary are received.
- Microscopes: Optical as well as Scanning Electron Microscopes (SEM) can be used for optical analysis and reverse engineering. Although chip feature sizes are well below one micron but they can still be seen with a good optical microscope and it may be even possible to reverse engineer hardware scramblers, crypto engines or hard-wired ROM. Automated tools can reconstruct complete circuits, or operating system source code from the ones and zeroes in a ROM mask. Voltage Contrast is a SEM application that can see high and low power values on the chip wires. A carefully prepared chip that is still capable of performing its electronic functions can be analyzed to reveal active sections in the chip and potentially even running code or passing data values.
- Probe Stations: This type of equipment allows tiny probe needles to be positioned on wires on a naked chip. Provided that a chip is still performing its electronic functions it is possible to create new channels to the outside world. Even though it is tedious but if the data bus can be located, probe needles may be able to tap all data exchanges between the CPU and the memories. In combination with a logic analyzer it is possible to retrieve full running program code and program data including keys. Vice versa it may also be possible to force a wire to accept data that effectively overrules the original data. In that manner microinstructions can be changed so as to cause the processor to take a complete different execution path with all possible consequences. In such a manner the entire code can be monitored or sometimes even edited.
- Focused Ion beam (FIB): This variation on a Scanning Electron Microscope shoots ions instead of electrons and is not only able to make small details visible, but also to make changes to circuit board. By adding different gasses to the ion beam it is possible to deposit material that creates wires, insulators or even semiconductors. This way blown fuses of test circuits can be reconnected, or hidden internal signals can be forwarded to external wires. In multi-layer chips it may be possible to surface ‘buried’ wires by creating a sort of tunnel. Also wires that are too thin and fragile to put probe needles on can be strengthened and enlarged to form a probe pad by putting on extra material with the FIB. Although physical attacks are extremely powerful they also have a disadvantage: they are invasive and often destructive. As the attacker can often not re-use the device it is not always an attractive approach. Also, these instruments are quite expensive and require a lot of skill.

## COUNTERMEASURES AGAINST PHYSICAL ATTACKS

Chip manufacturers have attained a significant improvement in physical security over the most recent years. This is a remarkable change. It is only a couple of years ago that retired machines from regular chip production were in general used to make smartcard chips. This was caused by the low chip prices and limited functionality needed for the chips. Today the smartcard market is a mass market and functional complexity has grown hugely. For that reason manufacturers can afford to use new advanced equipment and highly sophisticated chip designs. Specific areas of improvement are:

- Feature Size: In 5 years' time the size of transistors and wires on the chip surface has shrunk from more than 1 μm to less than 200 nm. This size is too small for optical microscopes to analyze and too small for probe stations to put needles on. Sophisticated microscopes and Focused Ion Beams can still work on this size.
- Multi-Layering: Today's smartcard chips use multiple layers. Not only is the number of semiconductors that can be produced, larger, but also is it also possible to hide sensitive data lines underneath other layers that contain less sensitive connections. This leads to an increase in security of the sensitive data.
- Protective Layer: In order to prevent analysis of live data processing it is possible to use a top layer that contains an active grid carrying a protection signal. Interruption of that signal will cause the chip to erase its memories and halt. However, skilled attackers might still be able to make a bypass through the grid and then penetrate the protective layer. Therefore, advanced grids would use a large number of seemingly non-correlated and frequently changing signals. This will significantly reduce the attacker's ability to access underlying lines by means of FIB modifications. Many low level hackers can be side lined by implementing this process.
- Sensors: Signals that measure environment variables such as light, temperature, power supply and clock frequency can be used to disable the chip as soon as out-off-bound conditions are detected. This will reduce the attacker's possibility to do live data analysis on a prepared chip. On the other hand they may also affect the reliability of the chip and for that reason be tuned quite fault-tolerant. These sensors help in protecting data but they are also prone to hijacking.
- Bus Scrambling: The data bus between various building blocks (e.g. processors and memories) can be scrambled using a sophisticated non-constant scrambling technique. An attacker attempting to interpret the bus data needs to do a full reverse engineering of the scrambler logic.
- Glue Logic: Instead of placing functional blocks in separate sections on the chip it is also possible to mix it all up and create glue logic. This way an attacker will no longer be able to easily identify the functional building blocks by analyzing the physical structures on the chip. Altogether there are many ways to reduce the possibilities of physical attacks to succeed. Nevertheless not all manufacturers use all of these options, or use them only for their most advanced and expensive devices. Many smartcard chips existing on the market today do not yet benefit from the newest technological advances. It is noteworthy that analysis techniques are improving as well and becoming more accessible.

## SIDE CHANNEL ATTACKS

Despite the complex chip designs we have to realize that integrated circuits are just a whole bunch of switching semiconductors. These semiconductors are sensitive to basic physical phenomena like electric power, radiation and voltage fluctuations. Although the chips are designed to process programmed stimuli and communicate only via restricted channels, they are in fact quite sensitive to variations in their environment. They also produce signals apart from those that were intended. These side signals may not give away the responses or abstracts of the secure data, but then can lead to leak in the security of the smart card.

Side Channel Attacks are attacks that use these physical phenomena to analyze or manipulate the behavior of a smartcard chip. Although they are related to the physical attacks that were discussed before, they are essentially different in operation because they are non-invasive. Side Channel Attacks can be practiced without physically opening the device and without damaging it.

Side Channel Attacks can be broadly divided into:

- Side Channel Analysis
- Side Channel Manipulation

Some physical phenomena's that can be used for Side Channel Analysis are described below:

- Power Consumption: Semiconductors use electric current during operation. The total amount of power consumed by a chip is very much dependent on the ongoing process. Measurement of the power consumption can reveal detailed information about the information being processed.
- Electromagnetic Radiation: Every switching transistor produces a bit of electromagnetic radiation. Just like power consumption this information can in theory provide a complete picture of the ongoing processes.
- Time: Microprocessors need time to complete their tasks. The amount of time may be variable and related to process parameters.

Physical phenomena that can aid Side Channel Manipulation by disturbing electronic circuits are:

- Voltage: most electronic circuits are designed to operate from a defined and constant supply voltage. Sudden changes to the power supply (power glitches) may change the behavior of the chip and trigger alternative behavior.
- Electromagnetic Radiation: A strong electromagnetic pulse can induce signals into the chip wires that may damage the chip, but also change its behavior.
- Temperature: electronic devices have a limited temperature range for operation. Outside the boundaries it may be possible to change their behavior.
- Light and X-Rays: semiconductors are sensitive to light. A suitably directed beam of light will affect a region of a chip, possibly resulting in behavior changes.
- Frequency: microprocessors are designed to operate within a nominal clock frequency range. Above the maximum frequency switching errors may occur in complex instructions that need a bit more time. A very low frequency (or even single stepping) may also offer interesting observations to an attacker.

There are two attacks that are very common:

- Differential Power Analysis – a statistical attack on a cryptographic algorithm, which compares a hypothesis with a measured outcome and is often capable of extracting an encryption key from a smart card or other computing device□

- Power Glitching – microprocessors are designed to operate from a stable voltage wherein interruptions of the power supply are likely to crash running applications or reset the circuit. A power glitch will affect both the stored and the threshold values. Different internal capacities will cause the values to be influenced differently, possibly resulting in a misinterpretation of the actual value.

## COUNTERMEASURES FOR SIDE CHANNEL ATTACKS

There are three levels of defense developed:

- Hardware Countermeasures: Hardware countermeasures reduce the susceptibility to side channel analysis. It reduces the signal to noise ratio, thus, make attacks more difficult to occur.
    - Balance the circuits and reduce electromagnetic emissions to lower the power signal.
    - □Perform concurrent random processes to increase noise level amplitude.
    - Process interrupts and variable clock speeds are introduced with timing noise to prevent or hamper alignment of traces.
- Software Countermeasures: Software countermeasures decrease the signal to noise ratio to reduce the emission of useful information from the side channels.
    - Perform random process ordering for parallel algorithm substitutions to reduce relevant signals.
    - Perform random delays or alternating paths to add timing noise that will hamper the alignment of traces, and deteriorate the quality of the differential trace.
    - Implement time constant key operations to eliminate time dependencies in key material and intermediate values avoiding simple power analysis by visual inspection of traces.
- Application Level Countermeasures like:
    - PIN verification blocks after three successive error scan be a useful protection against differential analysis.
    - Input and output visibility of cryptographic algorithms should be limited or restricted to avoid attackers to perform a differential analysis.

## CONCLUSIONS

In this paper we have discussed about the security issues and methods used to minimize the different categories of threats. Each category differs into some characteristics and dangers. The possibility of achieving practical smartcard security is achieved regardless of all the threats and attacks.

A regular study on the emerging threats should be considered to ensure the security to be maintained at a desired level.

## ACKNOWLEDGEMENTS

Syscom Corporation Ltd supported this work.

## REFERENCES

1. Smart Card Security User Group, Smart Card Protection Profile Draft, Version 2.0, 1.5.2000
2. eESC TB6 Contactless Smart Cards, "Contactless Technology Threat Evaluation Report", CSv2 Vol 6 Part 2 □
3. "Java Card Technology Overview", Chapter 3.
4. Jacques Fournier. Security attacks, countermeasures and testing for smart cards. Presentation in the MSc in Information Security, February 2008.
5. S.M. Sze: Semiconductor Devices - Physics and Technology. John Wiley & Sons, 1985□
6. B. Schneier, A. Shostack, “Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards”, USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, May 10–11, 1999.□