A Review of Smartcard Security Issues

Hoon Ko[1] and Ronnie D. Caytiles[2]

Abstract

The term "Smartcard", is widely used for business transactions and multiple services and are specifically designed for security, thus, it incorporates mechanisms for detection of and recovery from security problems. This technology can provide identification, authentication, data storage and application processing. This paper presents an overview of the Smartcard technology and the threats to its security categorized as Logical, Physical, and Side Channel. The dangers caused by these threats are discussed along with its basic countermeasures.

Keywords : Smartcard, Logical Threats, Physical Threats, Side Channel Threats.

1. Introduction

Smartcard evolved from very simple phone cards to business cards made with inferior equipment into complex high technology security solutions that can now support a large number of applications. Smartcard usage is rigorously growing over the last decade as they are being used in telecommunications (GSM), banking services and various other areas.

Security features of previous smartcards are limited to a mechanism preventing the chip on the card to be filled up again. Thus, its use is limited into a memory chip that can hold a stored value which is described as write once only. These early smartcards were disposable and used as stored value cards for payphones.

Today's applications require more functionality and security and are much more complex. Today's smart cards are re-usable, hold large quantities of data, speed transaction times, identify the cardholder, and even provide loyalty benefits. Smartcards are now equipped with microprocessors and a significant number of security measures

The self-containment of Smartcards makes them resistant to attack as they do not need to depend upon potentially vulnerable external resources. Because of this, Smart Cards are often used in applications which require strong security protection and authentication. Smart cards may also provide strong security authentication

Received(March 28, 2011), Review request(March 29, 2011), Review Result(1st: April 12, 2011, 2nd: April 28, 2011)
Accepted(June 30, 2011)

[1]GECAD ,ISEP, IPP, Rua Dr. Antonio Bernardino de Almeida, 431,4200-072, Porto, Portugal
email: hko@isep.ipp.pt

[2](Corresponding Author) 306-791 Department of Multimedia Engineering, Hannam University
email: rdcaytiles@gmail.com

for single sign-on (SSO) within large organizations. Despite of the vulnerabilities displayed by Smartcards, designers of secure applications still use smartcards as one of the major technology for business transactions.

This paper gives a technical overview of the smartcard technology and threats in smartcard security. The hardware and software designs of Smartcard are outlined, then the different threat categories and their countermeasures are discussed.

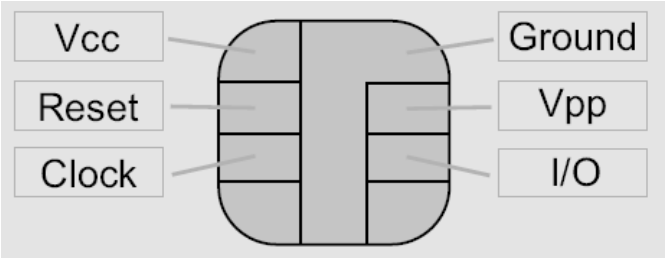
2. Smartcard Technology

A smart card or a chip card is a pocket-sized card with embedded integrated circuits which contains volatile memory and microprocessor components. Smart cards can provide identification, authentication, data storage and application processing [2].

The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contact-less smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card [5].

2.1. Hardware Architecture

Smartcards come in different shapes and could either be contact cards and contact-less cards. Contact smartcards are recognized by the characteristic contact stamp that appears on both credit-card sized and SIM card sized versions. The contact-less smartcards are more difficult to identify because the chip may be hidden not only inside a credit-card sized container, but also in badges, car keys or labels [1].

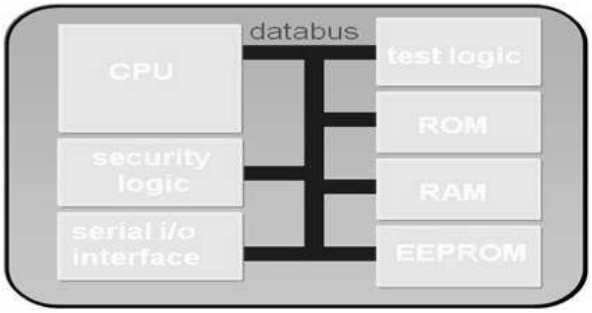


[Fig. 1] Contact Card Connections

In contact-less smartcards, users do not need to insert their contact-less smartcard into the slot of a smartcard reader. The communication takes place via radio frequency link, over the air, rather than through electrical contacts located on the smartcard module. It uses electromagnetic induction to provide power from

terminal to smartcard as well as for bi-directional data exchange.

Connections of a contact smartcard are shown in Figure 1. It is powered by through Vcc and Ground contacts of the chip. The Reset contact facilitates a hard restart of all processes. The clock contact provides an external clock signal to the chip that serves as the heartbeat for the internal processes. The Vpp contact originally provided a higher EEPROM programming voltage, and the I/O contact is a serial channel for bi-directional communication between smartcards and terminals.



[Fig. 2] Basic Smartcard Chip Architecture

The basic smartcard architecture is shown on Figure 2. It is a complete set of a microcontroller. It is a small embedded computer, shaped as a credit card or a SIM card with low processing power (8-bit CPU, 5 MHz clock) and small memory (4 Kb RAM, 16 Kb EEPROM, 64 Kb ROM).It is secure and inexpensive. Smartcard components are the following:

- CPU (Central Processing Unit): the heart of the chip, all computational work and data exchange goes via this function. Sometimes a cryptographic coprocessor is included. Most smartcard CPUs run on a clock frequency of 3.57 MHz.
- TestLogic: a verification function only used during the production process to test all internal circuits for manufacturing faults. Used to perform self-test procedures.
- Security Logic: a continuous function that checks environmental or abnormal conditions that could jeopardize the security of the smartcard, e.g. low voltage.
- I/O Interface: a communication function that takes care of receiving external commands and sending back responses using a serial communication protocol. Serves as the contact to the outside world
- ROM: the permanent memory of the chip. It can contain parts of the operating system and self test procedures. The memory size is typically 16, 32 Kb.
- RAM: the CPU's scratch pad memory. This is used for storing temporary or intermediate data like session keys, internal variables and stack data. The memory size is typically 512, 1 Kb. Known as the 'scratch pad' of the processor.

- EEPROM: non-volatile updateable memory. It is used for storing application data like keys, PINs, balances, phone numbers and sometimes application or even operating system code. Typically 8, 32 Kb.
- Data Bus: the transfer channel within the chip. All information exchanged between the various functions passes through this channel. The connection between elements of the chip. Typically 8 or 16 bits wide.

2.2 Software Architecture

Smartcard uses modular software designs and application separation. Smartcard operating systems uses life-cycle management that restricts the actions that can be performed in the smartcard. Data stored within a smartcard is organized in a nested file system. Files and directories together with the application data are stored in the EEPROM.

One popular smartcard operating system is the Java Card [4] that uses proven security concepts from the Java language. This operating system allows for flexible application design. Applications can be developed and loaded after card manufacturing or even post-issuance.

Communication via terminals is done through commands. Some basic commands are:-

· SELECT: open a file or directory.
· READ: read a file
· UPDATE: change the contents of a file
· AUTHENTICATE: authenticate the smartcard to the external world
· VERIFY: check a cardholder's PIN code.

Access with data contents on smartcards are protected with access conditions. It can only be read or written as long as the required PINS are verified or authenticated.

3. Aspects of Smartcard Security

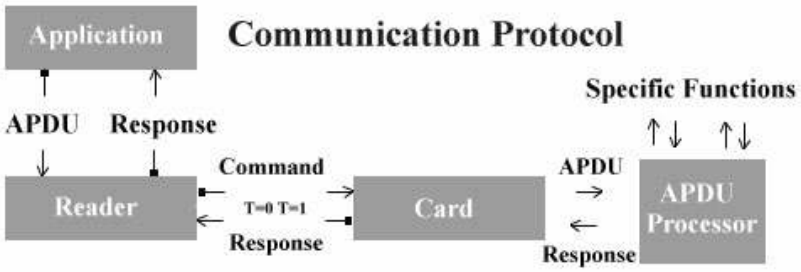
3.1 Smartcard Communications

A Smartcard and a Smartcard Reader communicate via means of small data packets called APDUs (Application Protocol Data Units). They use a mutual active authentication protocol to identify each other. The card generates a random number and sends it to the reader, which encrypt the number with a shared encryption key before returning it to the card. The card then compares the returned result with its own encryption. The pair may then perform the operation in reverse.

Once communication is established, each message between the pair is verified through a message authentication code. This is a number that is calculated based on the data itself, an encryption key, and a

random number. If data has been altered (for any reason, including transmission errors) message must be retransmitted. Alternatively, if the chip has sufficient memory and processing power, the data can be verified through a digital signature.

Cards and CADs communicate via a special instruction set. However, every external device communicating with the card makes it more vulnerable to attack via the communication link.



[Fig. 3] Smartcard Communication Protocol

3.2 Hardware

Unusual voltage supplies modify the contents of smartcards (data, keys, etc…) which is actually stored in the EEPROM. Physical attacks to smartcards are most destructive, in a way that smartcards can be cut and the processor removed. Security locks on smartcards can be removed by severe heating on the controller and exposing the EEPROM to UV light. To address this issue, some security processors implemented sensors for environmental changes.

3.3 Operating System

Data on Smart Cards is organized into a tree hierarchy which resembles a common OS. This has one master file (MF or root) which contains several elementary files (EF) and several dedicated files (DF). DFs and MF correspond to directories and EFs correspond to files, analogous to the hierarchy in any common OS for personal computers. DF's, EF's and MF's header contains security attributes resembling user rights associated with a file/directory in a common OS. Any application can traverse the file tree, but it can only move to a node if it has the appropriate rights.

There are five basic levels of access rights to a file (both DF and EF).

· Always (ALW): Access of the file can be performed without any restriction.

· Card holder verification 1 (CHV1): Access can only be possible when a valid CHV1 value is presented.

· Card holder verification 2 (CHV2): Access can only be possible when a valid CHV2 value is presented.

· Administrative (ADM): Allocation of these levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority.
· Never (NEV): Access of the file is forbidden.

CHV1 and CHV2 correspond to the two security PINs stored in the card: one is common user identification PIN and the other is a specific unblocking PIN pre-stored in the card. The OS blocks the card after a wrong PIN is entered several consecutive times. The number of times is fixed and depends on the OS. Once blocked, the card can only be unblocked with a specific unblocking PIN stored in the card. The unblocking PIN can become blocked in the same way. If this happens, card is said to be in irreversible blockage and may have to be scrapped for security reasons.

3.4 Software

Smartcard software producers provide their products with properly encrypted data and transfers. Theyhave developed hardware based or OS based instructions and libraries that support cryptographic algorithms.

4. Smartcard Security Threats

Since the popularity of Smartcard has emerged, they become popular targets for attackers. Smartcard security threats are classified as follows [7]:

· 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.
· Other Attacks

4.1 Logical Attacks

Smartcards uses a serial interface to issue commands for smartcards to perform. It supports a number of command options that flows into a single communication channel to exchange data with a smartcard reader. Confidentiality of data and undesired data modifications is critical to logical attack threats.

· Hidden Commands –smartcard operating systems cater a number of commands that can be abused to retrieve data from or modify data within the smartcard. These commands can remain active from an initialization phase or execution of a previous application.
· Parameter Poisoning and Buffer Overflow – misinterpreted disallowances on the parameters of commands could lead to surprising results.

· File Access – smartcard file systems have detailed permissions on files and directories. The command access permissions determine the security procedures to access a file. Access permissions can be confusing to smartcard operating systems with complex interactions.
· Malicious Applets – smartcard security can be compromised with rouge applets.
· Communication Protocol – information exchange between smartcard and terminal is dictated by a communication protocol that handles data flow control and error recovery.
· 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.

4.2 Physical Attacks

Physical attacks refer to the hardware abuse of smartcards. The functions encapsulated on the chip can be reversed engineered, although, may require high-end lab equipment.

· Chemical Solvents, Etching and Staining Materials –smartcards can be de-layered and de-capsulated by etching materials. Etching dissolves the metal and silicon layers of the chip. 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.
· Microscopes – optical and Scanning Electron Microscopes (SEM) can be used for optical analysis and reverse engineering. A 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 – allows tiny probe needles to be positioned on arbitrary wires on a naked chip to create new channels to the outside world. All data exchange between the between the CPU and the memories can be tapped and it is possible to retrieve full running program code and program data including keys.
· Focused Ion beam (FIB) – it shoots ions that can make changes with the circuitry. Blown fuses of test circuits can be reconnected, or hidden internal signals can be forwarded to external wires.

4.3 Side Channel Attacks

Smartcards are designed with integrated circuits that are composed of switching semiconductors which are sensitive to basic physical phenomena like electric power and radiation. Side Channel Attacks [6] uses physical phenomena to analyze or manipulate the behavior of a smartcard chip. These attacks are practiced without physically opening the device and without damaging it.

· 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 [3].

· 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.

4.4 Other Attacks

Some other threats are identified as:

· Eavesdropping – easy ways to intercept and alter data being transmitted over the air.

· Interruption of operations – The communication between the reader and the card may be interrupted any time without notice

· Denial of service – cards can be emptied or destroyed remotely using inappropriate electronic waves

· Covert transactions – fake transactions triggered by fraudulent merchants using fake readers

· Communication links and dual modes – dual mode chip cards tend to share the underlying chip so that the only difference is the way the data is transmitted to the I/O buffer of the chip card.

5. Smartcard Security Threats Countermeasures

5.1 Countermeasures for Logical Attacks

Logical attacks are dependent with the smartcard software complexity. The number of bugs grows with the size of the software code. The following are identified as countermeasures to address these issues:

· Structured Design – create software in small functional building blocks that can more easily be understood and validated.

· Formal Verification – use mathematical models to prove the soundness of functions.

· Testing – perform experimental validation of the implementation.

· Standardization of Interfaces and Applications – re-use of proven 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.

· Popularity of Evaluation Labs – a growing number of card manufacturers and card issuers use evaluation labs to get a (formal) report or certificate.

The growing software complexity always brings the risk of introducing new flaws. Careful design and validation may reduce the number and increase the difficulty of exploiting the flaws.

5.2 Countermeasures for Physical Attacks

High sophisticated chip designs are accompanied with significant improvement in physical security.

- Feature Size –the size of smartcards are relatively becoming smaller for optical microscopes to analyze and too small to put needles of probe stations.
- Multi-Layering –it is possible to hide sensitive data lines underneath other layers that contain less sensitive connections for multiple layer chips.
- Protective Layer –using a top layer that contains an active grid carrying protective signals prevent analysis of live data processing. A large number of seemingly non-correlated and frequently changing signals can avoid penetration of the protective layer.
- 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, thus, reducing the attacker's possibility to do live data analysis on a prepared chip
- Bus-Scrambling – the data bus between various building blocks (e.g. processors and memories) can be scrambled using a sophisticated non-constant scrambling technique.
- Glue Logic – creating glue logic or mixing all functional blocks can confuse attackers in identifying the functional building blocks and analyzing the physical structure of the chip.

5.3 Countermeasures for Side Channel Attacks

There are three levels of defense developed against Power Analysis and other types of Side Channel Analysis attacks.

5.3.1 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.

5.3.2 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.
- Add random values to be subtracted later to blind intermediate values to prevent useful information leakage. These are carefully designed to compensate the deviation caused by random values.

5.3.3 Application Level countermeasures

Some general simple countermeasures that can deny the requirements for side channel analysis are:

- PIN verification blocks after three successive errorscan 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.

5.3.4 Countermeasures for Power Glitching

The rigid use of sensors for voltage, frequency and temperature is the most common strategy against power glitching attacks. But then, sensor setting affects the reliability and potentially causing malfunctions in some terminals or climates of smartcards.

Software and application countermeasures are to be implemented to detect and recover from fault injection. Checking the crucial program flow decisions and cryptographic results carry out the fault detection. The validity of results is done by computing the results twice and comparing both results.

5.4 Countermeasures for Other Attacks

Users should be aware of the properties of Smartcards to address the threats accordingly. Public Key Cryptography and crypto-coprocessors needs to be optimized to fit the card. Encryption of the data being exchanged and mutual authentication is a must.

6. Conclusion

The study outlined the basic concepts of Smartcards as it is widely used for business transactions and multiple services. Smartcards are specifically designed for security, thus, it incorporates mechanisms for detection of and recovery from security problems. It is a pocket-sized card with embedded integrated circuits that contains volatile memory and microprocessor components. It can provide identification, authentication, data storage and application processing. Smartcard security threats and some basic countermeasures are identified into three categories: Logical, Physical and Side Channel. 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.

References

[1] eESC TB6 Contactless Smart Cards, "Contactless Technology Threat Evaluation Report", CSv2 Vol 6 Part 2, Available at: http://dematerialisedid.com/PDFs/OSCIE/Download/06-2.PDF

[2] Department of Finance and Deregulation, Australian Government, "National Smartcard Framework", December 2008, Available at: http://www.finance.gov.au/e-government/security-and-authentication/docs/smartcard-handbook.pdf

[3] Paul Kocher, Joshua Jaffe and Benjamin Jun, "Differential Power Analysis", in proceedings of Advances in Cryptology, CRYPTO '99, Springer Verlag, 1999. Available at: http://www.cryptography.com/public/pdf/DPA.pdf

[4] "Java Card Technology Overview", Chapter 3, Available at: http://java.sun.com/developer/Books/consumerproducts/javacard/ch03.pdf

[5] http://en.wikipedia.org/wiki/Smart_card

[6] Prof. Jean-Jacques Quisquater, Math RiZK, "Side channel attacks",October 2002, Available at: http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_ report.pdf

[7] Ahmadou A. SERE, Julien Iguchi-Cartigny, Jean-Louis Lanet "Evaluation of Countermeasures Against Fault Attacks on Smart Cards", IJAST Vol.4, No.1, April, 2011

Author

Hoon Ko

Ph.D. School of Computing, Soongsil University, S Korea, August 2004.

MS. School of Computing, Soongsil University, S Korea, February 2000nBS. Department of Computer Science, Howon University, Gunsan, S Korea, February 1998.

Doctor Researcher GECAD , ISEP, IPP.

Rua Dr. Antonio Bernardino de Almeida, 431,4200-072, Porto, Portugal

Ronnie D. Caytiles

1995 − 2000: Bachelor of Science in Computer Engineering, Western Institute of Technology, Iloilo City, Philippines

Currently: Integrated Course for M.S. and Ph.D. in Multimedia Engineering, Hannam University, Daejon, Korea.

Research Interests: Information Technology Security, U-Learning, Control and Automation