SMARTCARD SECURITY

Y.Sowparaniga[1], K.Hema[2], T.Suganya[3], J.Joselin[4]
[1,2,3]III M.Sc Software Systems,
[4]MCA.,M.Phil., Assistant Prof.,
Sri krishna arts and science college, coimbatore-8

Abstract **- Smart cards provide computing and business systems the enormous benefit of portable and secure storage of data and value. At the same time, the addition of smart cards into your system introduces its own security management issues, as people contact card data far and wide in a variety of applications.**

Index Terms**- Smart Card, Integration, security.**

I. INTRODUCTION

The self-containment of Smart Card makes them resistant to attack as they do not need to depend upon potentially weak external resources. Because of this, Smart Cards are often used in applications which require strong security fortification and validation.

Technology and security are strongly related. Crackers find sophisticated ways to get at apparently secure data on cards => Manufacturers have to come up with more sophisticated locks and keys on cards => Crackers come up with improved technique to go around these ... thus forming an infinite improvement loop, with both side motivating each other to use and create improved technology.

There are four diverse aspect of the Smart Card security:

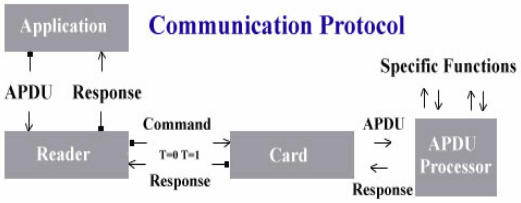
- Communication
- Hardware
- Operating System
- Software

II. COMMUNICATION

A Smart Card and a Card Accepting Device (CAD) be in touch via means of small data packets called APDUs (Application Protocol Data Units). The next individuality of this interaction makes it harder for third parties to attack the scheme effectively:

- Small bit rate (9600 bits per second) by means of a serial bi-directional transmission line (ISO standard 7816/3)
- half duplex method for transferring the information (facts simply transfers in one direction at a time)
- The communication follow a complex protocol, described below.

However, every exterior device communicating with the card makes it weaker to attack via the communication link.



Through a message confirmation code. This is an integer that is calculated based on the data itself, an encryption key, and a random digit. If data has been distorted (for any reason, together with broadcast errors) message should be retransmitted. On the other hand, if the chip has enough memory and processing power, the data can be demonstrated through a digital signature.

The most widespread encryption method are symmetric DES (Data Encryption Standard), 3DES (triple DES) and public key RSA (The Smart Card and the CAD use a shared active verification protocol to recognize each other. The card generate a random number and sends it to the CAD, which encrypt the digit with a shared encryption key previous to recurring it to the card. The card then compares the returned outcome with its own encryption. The couple may then execute the process in reverse.

Once message is established, each message between the couple is proved Rivest-Shamir-Adleman's algorithm), allow up 56, 168, and 1024 bit

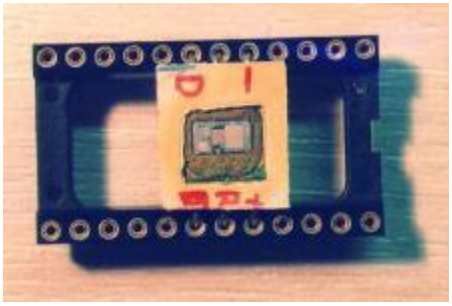
long keys, correspondingly. Sadly, these keys are not indestructible. The couple managed to crack the Dallas DS5002FP Secure Microcontroller, explained at the occasion by one European signals intelligence agency as the most protected processor accessible on all-purpose sale. They used brute force methods on a PC improved with a pair of hundred dollars of extra hardware!

Cards and CADs converse via a special order set. For example, the Schlumberger Reflex 60 instruction set contains:

0x60	**Gets reader type and activate reader**
0x61	Sets reader with ICC communication parameters
0x62	Turns card power ON
0x63	Turns card power OFF
0x64	Sends RESET signal to card
0x65	Gets reader-card status
0x66	Sends one byte to reader
0x67	Sends data block to reader
0x68	Makes reader resend last data block
0x69	Gets reader capabilities
0x6A	Deactivate reader
0x6B	Activate reader-dependent features
0x6C-0x6F	Reserved

III. HARDWARE SECURITY

Problems

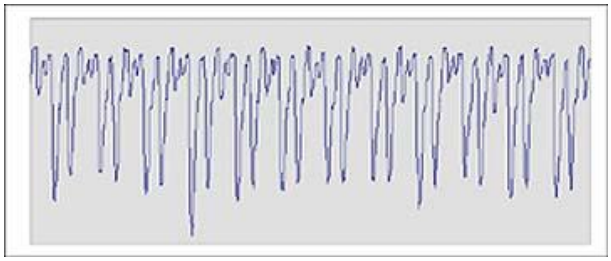


All data and password on a card are saved in the EEPROM and can be erased or customized by an unusual power supply. Therefore some safety processors execute sensors for ecological changes. However, since it is thorny to find the right level of sympathy and there is a voltage oscillation when the power is abounding to the card, this technique is not extensively used. Other winning attacks techniques include heating the controller to a high temperature or focus the UV light on the EEPROM, thus removing the safekeeping lock. Persistent physical attacks are the most caustic when the card is cut and processor detached. Then the layout of the chip can be repeal engineered.

Differential Power Analysis (DPA), is an arithmetical attack on a cryptographic algorithm which compare a theory with a deliberate outcome and is often proficient of extracting an encryption key from a smart card or other computing device. Simple Power Analysis (SPA), the straight analysis of the recorded authority data to decide actions and data, is also functional.

Solutions

Several technologies have been urbanized to

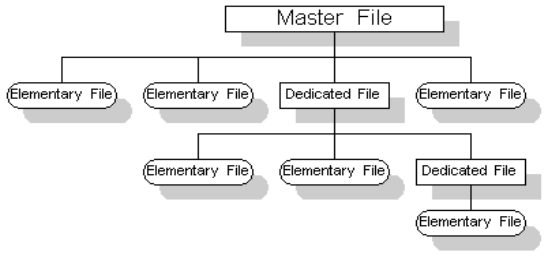


defend Smart Cards. These are methods of ST Microelectronics against SPA/DPA attacks:

- *Technology barrier*. Superior 0.6 micron expertise greatly reduces the size and voltage use of cards as well as the relative variation in their operating parameter. This makes it very hard for exterior SPA/DPA methods to distinguish between usual card fluctuations and data-related fluctuations.

- *Clock fluctuation.* A special Clock Software administration facility, when correctly used, results in extremely variable software timing when the implanted application program is resulting.
- *Unpredictable behavior.* A built-in timer with suspend ability and an impulsive Number Generator is used to impose irregular variations on software implementation behavior, with resulting changes in the prototype of power consumption.
- *Robust design.* A modular plan allows new hardware variation, counting custom variations, to be formed swiftly and competently, thereby allowing fast response to new attack scenario.
- *Memory control for multi-applications.* An improved Memory Access Control structure provides safe operating system support for multi-application cards.
- *Security mechanisms and firmware functions.* An improved set of security mechanism and firmware function allow the application to notice and react suitably to the incidence of conditions that might designate an attack. These circumstances include invalid in commission conditions, bad opcodes, bad address and infringement of chip reliability; the possible responses include disrupt, program reset, immediate removal of all RAM data and flash encoding of the entire EEPROM array.

IV. OS SECURITY



Data on Smart Cards is prearranged into a tree hierarchy. It has one master file (MF or root) which contain some elementary files (EF) and number of dedicated files (DF). DFs and MF correspond to directories and EFs correspond to files, parallel to the chain of command in any common OS for PCs. However, these two hierarchies fluctuate in that DFs can also include data. DF's, EF's and MF's header contains safety attribute resembling user authority connected with a file/directory in a common OS. Any application can pass through the file tree, but it can only move to a node if it has the proper rights.

Attributes (Access Rights)

There are five essential levels of access rights to a folder (both DF and EF). Some Operating System provides additional levels.

Essential levels can be classified, gradually more in security, as follows:

1. **Always (ALW):** Access of the file can be performing without any limit.
2. **Card holder verification 1 (CHV1):** Right of entry can only be probable when a legal CHV1 importance is presented.
3. **Card holder verification 2 (CHV2):** Right to use can only be possible when a valid CHV2 value is offered.
4. **Administration (ADM):** Allowance of these levels and the particular necessities for their completion are the liability of the appropriate organizational power.
5. **Never (NEV):** Right of entry of the file is prohibited.

Though, presenting a CHV2 does not be sufficient to access a file requiring CHV1. CHV1 and CHV2 keep in touch to the two defense PINs stored in the card: one is widespread user recognition PIN and the other is an exact unblocking PIN previously stored in the card.

The PINs

The PINs are stored in separate simple files, EF_{CHV1} and EF_{CHV2} for example. The Operating System block the card behind a wrong PIN is entering several successive times. The number of times is fixed and depends on the Operating System. Once infertile, the card can only be unblocked with an exact unblocking PIN stored in the card. The unblocking PIN can turn into blocked in the similar method. If this happen, card is said to be in irreparable obstruction and may have to be scrapped for protection reasons.

If the PIN is blocked, the feature of every file is distorted to require CHV1. After the unblocking PIN is obtainable, the file attribute are returned to regular, the counter for the PIN is set rear

to its maximum value and the oppose for the unblocking PIN is decreased. If the latter counter value reaches zero, it cannot be used for unblocking the PIN any further. This provides supplementary defence for the card.

V. SOFTWARE SECURITY

Software producers also make a payment to the Smart Card security - they ought to provide their products with correctly encrypted data and transfers. To help them attain this goal, hardware-based or Operating System based commands and library sustaining superior cryptographic algorithms have been urbanized.

VI. CONCLUSIONS

The majority attacks today are categorized as class 3 attack, which means that either the costs linked to smash the system are extremely spare than the price of the system itself, or that the cracker has to expense numerous or hundred years of computing authority to crack into a solitary deal. Technology is mounting quicker than cracker method. Consequently, each new invention of technology typically prevents attacks that the previous invention.

REFERENCE

1. *https://en.wikipedia.org/wiki/Smart_card_security*
2. *http://www.smartcardbasics.com/smart-card-security.html*
3. *http://www.smartcardalliance.org/publications-smart-card-security/*
4. *http://people.cs.uchicago.edu/~dinoj/smartcard/security.html*