IMPROVING SECURITY THROUGH SMART CARDS

1.) S.BALAJI Professor, ECE DEPARTMENT

CMR GROUP OF INSTITUTIONS

2).Dr. HABIBULLAH KHAN DEAN(SW),

KL UNIVERSITY

3) K.ADITYA, ECE DEPARTMENT

CMR GROUP OF INSTITUTIONS

ABSTRACT

Almost a decade ago we all might have heard about the smart card and its role in the financial sector, especially for retail transactions. Smartcard provides a special security when compared to normal money transaction. But its implementation in the case of Retail payments has not been so popular. But it is found really useful in the area of transit payments and Personal Identification. But some other sectors like mobile telecommunication found this more useful and started using in Mobile phones as a Subscriber Identification Modules (SIM). In this paper we are trying to re evaluate the use of smart card and its importance in the financial transaction.

Introduction

A smart card is just – "a small chip integrated inside a plastic card". It is that one which can participate in an automated electronic transaction.It can also be defined as: "Smart cards are portable data cards, which should communicate withanexternal device to gain access to a display device or a network". Thus, they can be plugged into a card reader (also referred as card terminal), or they can operate using radio frequencies. The main purpose of the card lies in the security. It stores data's securely and can host/run a wide range of security algorithms and functions. Since the card cannot be forged or easily copied, it is mainly used for the security purposes. Smart card chips tend to be very small. The several types of cards which come under the category of Smart card are:

- Magnetic Stripe Cards
- Chip Cards

- Microprocessor Chip Cards.

Figure 1.: Different types of Smart cards

Smart Card Architecture

The smart card architecture is explained by using Physical characteristics, Electrical characteristics and their components as follows.

- **Physical Characteristics**

A smart card is no more than a piece of silicon in a piece of plastic.The manufacturing of smart cards consists of a silicon chip connected to a contact module, the whole being reported onto a plastic card body.

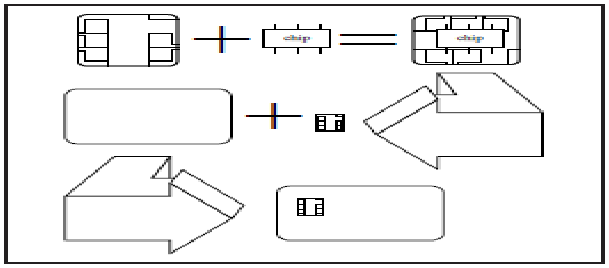

Figure 2.1: Smart card manufacturing

2.1 Electrical Characteristics

Electrical characteristics are defined by ISO/IEC 7816-3 (electrical interface and transmission protocol).Basically, most smart cards use an asynchronous serial transmission protocol, character oriented. The electrical interface is five contacts: Vccand GND (power supply), Reset(initialisation), Clock and I/O (serial interface)

2.2 Components of Smart Card

The components of a Smart card are:

- Small Microprocessor chip
- Plastic card
- CPU
- 3 Types of memory
- Interconnecting circuit

As discussed above, the Smart card will be having a small microprocessor chip inside a plastic card. It also has a CPU and 3-types of memory as well as the interconnecting circuitry. But, the device has no clock or in-built power supply. The three types of memory are: RAM, ROM and EEPROM.

2.3. Applications of Smart Cards

Smart cards are used in many current and real-world systems. It can be also used for many future applications. In fact the capability and numbers of cards are being increasing in just about all areas of use. Some of the growing applications include:

- Mobile telephony
- Banking (Master cards and Visa cards)
- Transport
- Identity cards/ Passports
- Satellite T.V. and
- Health cards

CHAPTER 3

Classifying the Attackers

The possible attackers can be divided to following categories:

- **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.

❖ 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.

- ❖ **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.

- ❖ **Attacks by the Cardholder against the Data**

3.2 Security

Security is basically the protection of something valuable to ensure that it is not stolen, lost, or altered. The term "data security" governs an extremely wide range of applications and touches everyone's daily life. Concerns over data security are at an all-time high, due to the rapid advancement of technology into virtually every transaction, from parking meters to national defence. Data is created, updated, exchanged and stored via networks. A network is any computing system where users are highly interactive and interdependent and by definition, not all in the same physical place.

3.2.1 The Elements of Data Security

In implementing a security system, all data networks deal with the following main elements:

- **Hardware**, including servers, redundant mass storage devices, communication channels and lines, hardware tokens (smart cards) and remotely located devices (e.g., thin clients or Internet appliances) serving as interfaces between users and computers
- **Software**, including operating systems, database management systems, communication and security application programs
- **Data**, including databases containing customer - related information.
- **Personnel**, to act as originators and/or users of the data; professional personnel, clerical staff, administrative personnel.

CHAPTER 4

The Mechanisms of Data Security

Working with the above elements, an effective data security system works with the following key mechanisms to answer:

→Data Integrity

This is the function that verifies the characteristics of a document and a transaction. Characteristics of both are inspected and confirmed for content and correct authorization. Data Integrity is achieved with electronic cryptography that assigns a unique identity to data like a fingerprint. Any attempt to change this identity signals the change and flags any tampering.

→Authentication

This inspects, then confirms, the proper identity of people involved in a transaction of data or value. In authentication systems, authentication is measured by assessing the mechanisms strength and how many factors are used to confirm the identity. In a PKI system a Digital Signature verifies data at its origination by producing an identity that can be mutually verified by all parties involved in the transaction. A cryptographic hash algorithm produces a Digital Signature.

→Non-Repudiation

This eliminates the possibility of a transaction being repudiated, or invalidated by incorporating a Digital Signature that a third party can verify as correct. Similar in concept to registered mail, the recipient of data re-hashes it, verifies the Digital Signature, and compares the two to see that they match.

→Card-Based System Security

These systems are typically microprocessor card-based. A card, or token-based system treats a card as an active computing device. The Interaction between the host and the card can be a series of steps to determine if the card is authorized to be used in the system.

CHAPTER 6

Conclusion

The smart card being most secure and proven for its security, but was not popular amount the payment schemes. The financial institutions were watching the developments in the area of smart card, until it get mature. Butinspite of its proven capability in the area of security, smart card failed to get enough popularity. One of the reasons of it is the lack of acceptance by the user. The penetrations of mobile device like mobile phone and PDA have made a significant impact in the area of e commerce. The mobile operators are also try to sell “Hard” their product by providing additional value added services. Even the Customer wants to have useful application in their mobile devices.

References

[1] American Express Express Pay - wwww.americanexpress.com/expresspay

[2] Master card paypass - www.mastercard.com/aboutourcards/paypass.html

[3] American Public Transportation (APTA) - www.apta.com

[4] www.erggroup.com

[5] www.alittleworld.com

[6] www.javacardforum.org

[7] http://www.smartcardalliance.org/

[8] http://www.gemplus.com/pss/banking/

[9]http://www.international.visa.com/footer/contact.jsp

[10] www.theruthgroup.com