Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.982 – 987

RESEARCH ARTICLE

Smart Card: Turning Point of Technology

Abhishek Mahajan, Akash Verma, Dhruv Pahuja

CSE Department, Dronacharya College of Engg.

CSE Department, Dronacharya College of Engg.

CSE Department, Dronacharya College of Engg.

mhjn01abhishek@gmail.com, akashverman@gmail.com, dpahuja46@gmail.com

Abstract: ***A smart card, chip card, or integrated circuit card (icc) is any pocket-sized card with embedded integrated circuits. Smart Cards are secure portable storage devices used for several applications especially security related ones involving access to system's database either online or offline. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene orpolycarbonate. This research is chiefly to study the security principals of smart card and assess the security aspects' affect on smart card technology adoption.***

Keyword: smart card, security, Integrity, Verification, Information Technology

I. INTRODUCTION

Smart cards have been utilized excessively during the last couple of decades. In recent years though, a new generation of smart cards evolved: programmable smart cards. In this paper the authors give an overview of the current state of the technology and compare the cards on the market. The scope of uses for a smart card has expanded each year to include applications in a variety of markets and disciplines. In recent years, the information age has introduced an array of security and privacy issues that have called for advanced smart card security applications.

In 1968 and 1969 German electrical engineers Helmut Gröttrup and Jürgen Dethloff jointly filed patents for the automated chip card (for details see page of Helmut Gröttrup). French inventor Roland Moreno patented the memory card concept in 1974. An important patent for smart cards with a microprocessor and memory as used today was filed by Jürgen Dethloff in 1976 and granted as USP

4105156 in 1978. In 1977, Michel Ugon from Honeywell Bull invented the first microprocessor smart card.

The first cards with magnetic stripes were developed by the International Air Transportation Association (IATA) in the 1970's. On this type of card the magnetic stripe stored 210 bit/inch of information, which means about 80 alphanumeric (7-bit) characters. For the sake of compatibility, today's magnetic stripes are divided into three regions. The first region corresponds to the original stripe, storing read-only information. The second region can hold additional 40 digits with an information density of 75 bit/inch. The third region is read-writeable and may contain 107 digits.

According to Eurosmart, worldwide smart card shipments will grow 10% in 2010 to 5.455 billion cards. Markets that have been traditionally served by other machine readable card technologies, such as barcode and magnetic stripe, are converting to smart cards as the calculated return on investment is revisited by each card issuer year after year.

A study by Dataquest in March, 2000, predicts almost 28 million smart card shipments (microprocessor and memory) in the U.S. According to this study, an annual growth rate of 60% is expected for U.S. smart card shipments between 1998 and 2003. Smart Card Forum Consumer Research, published in early 1999, provides additional insights into consumer attitudes towards application and use of smart cards. The market of smart card is growing rapidly due to its wide range of applications.

II. TYPES OF SMART CARDS

- Contact cards
- Memory Cards
- CPU/MPU Microprocessor Multifunction Cards
- Contactless cards
- Multi-mode communication cards
- Hybrid cards
- Dual interface cards
- Multi-component cards

III. MANAGEMENT OF MEMORY

Smart card is a device with major hardware constraints: low-power CPU, low data rate serial I/O, little memory etc. Today, card technology utilizes 8 bit processors (mainly of the 6805 or 8051 family) whose memory sizes are about a few tens of kilobytes (Urien, 2000), typically 1-4 kb RAM (Random Access Memory), 32-128 kb ROM (Read Only memory) and 32-64 kb EEPROM (Electrically Erasable Programmable Read Only Memory) at least, with options on FLASH and FRAM (Ferroelectric Random Access Memory) as well. As the demand for smart cards matures, the standard memory of 32 or 64 KBytes can prove a serious limitation.

Table: comparing size of different smart cards

Record description	External format		Internal format(bytes)	
	Size	Type	Size	Type
First Payment Card # (ISO)	19	N	10	BCD
First Payment Card Expiration Date	8	D	4	BCD
Second Payment Card # (non-ISO)	20	AN	20	ASCII
Second Payment Card Expiration Date	8	D	4	BCD

According to Junko (2002), the EEPROM used in current smart cards is reaching its scalability limits, particularly for alternative non-volatile memory for future smart cards. Currently Philips is leaning toward magnetic RAM as an alternative to EEPROM.

IV. CHIP SPECIFICATION

There are a number of factors to be decided in the specification of the integrated circuit for the smart card.For the purpose of this discussion we will consider a CPU based card although the manufacture of a memory card is substantially a subset of that described here. The key parameters for the chip specification are as follows,

- Microcontroller type (e.g 6805,8051)
- Mask ROM size
- RAM size3
- Nonvolatile memory type (e.g EPROM, EEPROM)
- Non volatile memory size
- Clock speed (external, and optionally internal)
- Electrical parameters (voltage and current)
- Communications parameters (asynchronous, synchronous, byte, block)
- Reset mechanism
- Sleep mode (low current standby operation)
- Co-processor (e.g for public key cryptography)

V. CARD SPECIFICATION

The specification of a card involves parameters that are common to many existing applications using the ISO ID-1 card. The following list defines the main parameters that should be defined,

- Card dimensions
- Chip location (contact card)
- Card material (e.g PVC, ABS)
- Printing requirements
- Magnetic stripe (optional)
- Signature strip (optional)
- Hologram or photo (optional)
- Embossing (optional)
- Environmental parameters

The characteristics of the smart card are part of the ISO 7816 part 1 (physical) and 2 (contact location) standards. The choice of chip location has been a difficult subject due largely to the use of magnetic stripes. The early French cards put the IC module further off the longitudinal axis of the card than the standard eventually agreed by ISO.

VI. PERFORMANCE

Performance and speed are very important factors that need to be considered in most smart card application. To achieve this, transistor scaling or the reduction of the gate length (the size of the switch that turns transistors on and off), must be taken into consideration.

Recently, IBM have built a working transistor at 6 nanometres in length which is per beyond the projection of The Consortium of International Semiconductor Companies that transistors have to be smaller than 9 nanometres by 2016 in order to continue the performance trend. The ability to build working transistors at these dimensions could allow developers to put 100 times more transistors into a computer chip than is currently possible. The IBM results will lead to further research into small, high-density silicon devices and allow scientists to introduce new structures and new materials.

VII. SECURITY

Smart cards have been advertised as suitable for personal identification tasks, because they are engineered to be tamper resistant. The chip usually implements some cryptographic. There are, however, several methods for recovering some of the algorithm's internal state.

As smart card is handicapped or highly restricted in their input/output (unable to interact with the world without outside peripherals), this leads to the involvement of many parties in its applications. Some of the parties involve: Cardholder, Data Owner, Card Issuer, Card Manufacturer, Software Manufacturer, and Terminal Owner as mentioned in (Schneier, 1999).

Smart cards can be physically disassembled by using acid, abrasives, or some other technique to obtain unrestricted access to the on-board microprocessor. Although such techniques obviously involve a fairly high risk of permanent damage to the chip, they permit much more detailed information (e.g. photomicrographs of encryption hardware) to be extracted.

VIII. BENEFITS

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/contactless 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. For example, a smart card can be programmed to only allow a contactless transaction if it is also within range of another device like a uniquely paired mobile phone. This can significantly increase the security of the smart card.

Individuals have better security and more convenience with using smart cards that perform multiple services. For example, they only need to replace one card if their wallet is lost or stolen. The data storage on a card can reduce duplication, and even provide emergency medical information.

IX. PROBLEMS

The plastic card in which the chip is embedded is fairly flexible. The larger the chip, the higher the probability that normal use could damage it. Cards are often carried in wallets or pockets, a harsh environment for a chip. However, for large banking systems, failure-management costs can be more than offset by fraud reduction.

If the account holder's computer hosts malware, the smart card security model may be broken. Malware can override the communication (both input via keyboard and output via application screen) between the user and the application. Man-in-the-browser malware (e.g. the trojan Silentbanker) could modify a transaction, unnoticed by the user. Banks likeFortis and Belfius in Belgium and Rabobank ("random reader") in the Netherlands combine a smart card with an unconnected card reader to avoid this problem. The customer enters a challenge received from the bank's website, a PIN and the transaction amount into the reader, The reader returns an 8-digit signature. This signature is manually entered into the personal computer and verified by the bank, preventing malware from changing the transaction amount.

Another problem is the lack of standards for functionality and security. To address this problem, The Berlin Group launched the ERIDANE Project to propose "a new functional and security framework for smart-card based Point of Interaction (POI) equipment".

X. SMART CARD OF THE FUTURE

Now let’s examine, what is realistic from the features of the ideal smart card, and what capabilities exist in the cards on the market today.

Today’s cards have 8-32 kilobytes of memory. This is likely to increase in the futurein parallel with the development of IC technology. Computational power has a closerlimit though. Controlling overheating has always been a problem in case of microelectronics but it case of cards the problem is even larger.

Real-time encryption of speech or video is far beyond the capabilities of today’s cards, and the authors believe that it will not be possible in the near future. Supplying cards with cryptographic hardware is a question of price thus it is a question of mass production. Security and portability are the two areas where cards can be better used than PCs. This is why the author suppose that the smart card of the future will be equipped with cryptographic hardware. The production of good quality random numbers is a problem yet to be solved. The documentation of today’s cards contains no information on the ways of random number generation.

CONCLUSION

Smart cards can add convenience and safety to any transaction of value and data; but the choices facing today's managers can be daunting. We hope this site has adequately presented the options and given you enough information to make informed evaluations of performance, cost and security that will produce a smart card system that fits today's needs and those of tomorrow.

Security is very crucial issue in smart card especially due to the various independent parties involve throughout the card’s life cycle leading to what is now called “splits” in trust. There is need to develop a method in which even without trust none of the parties can cheat one another. Further, to overcome the lack of security provided by passwords or PINs for authentication and access control, some researchers believe that biometric is the best genuine means of authentication.

The results of this study illustrate that security has an important and positive effect on user satisfaction and consequently on user acceptance. It means that with increasing the level of security, the level of user acceptance will be increased. Finally, further investigation needs to be carried out in the future to identify factors that will provide users better understanding of the system and also establish new techniques to increase the security level of the smart card.

REFERENCES

1. "Development of the "KAMICARD" IC card made from recyclable and biodegradable paper". Toppan Printing Company. Archived from the original on 2009-02-27. Retrieved 2009-03-27.
2. *Multi-application Smart Cards*. Cambridge University Press.
3. ***Smart Cards: More or 'Less. ABI/INFORM Global database.***
4. Smart Card License System
5. Octopus Card Benefits
6. Mozilla certificate store
7. Security Token/Smartcard Support used by FreeOTFE
8. "News Release - Smart card technology to monitor smart food choices in schools". Ifr.ac.uk. 2005-07-14. Retrieved 2014-02-13.
9. Smartcardalliance.org
10. http://www.smartcardbasics.com/
11. En.wikipedia.org

