SMART CARD SECURITY

PRESENTED BY

AVANI P (16)
CHAITHANYA PO V (17)
CHANDHAN M (18)
FATHIMA SHADHA SULAIMAN (19)
GOKULJITH K (20)

S2 ECB
GOVERNMENT COLLEGE OF ENGINEERING KANNUR

OUTLINE

1. introduction
2. about Smart card and working
3. security features of smart card
4. security principles of smart card
5. attacks on smart card
6. benefits and disadvantages
7. conclusion
8. reference

INTRODUCTION

We live in a smart world where technological trends and advancement are making life easier for everyone Smart cards are providing a safer and secure means of conducting financial transactions.Smart cards are now common in every economy across the world - they are being used by almost everyone that receives a paycheck. The idea of a smart card is to reduce the archaic manner in which people carry cash about and feel insecure owing to prying eyes and numerous cases of heists associated with moving large chunks of cash about.

INTEGRATED CIRCUIT CARD (smart card)

- these are the newest and most clever additions to the ID-1 family
- they also follow the details laid down in the ISO 78164 series
- cards with over 20 Kb of memory are currently available
- the stored data can be protected against unauthorized access and tampering
- Memory functions such as reading, writing, and erasing can be linked to specific conditions, controlled by both hardware and software.

COMPONENTS OF CONTACTLESS SMART CARD

smart pad

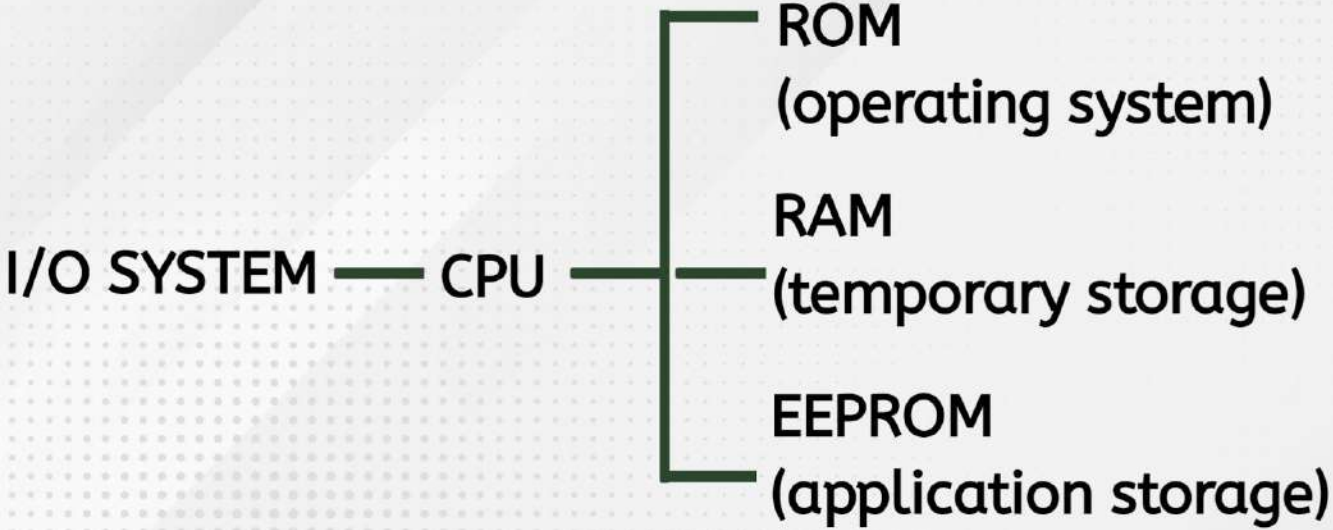
smart Card chip

plastic card layer

contacless inlay with antenna

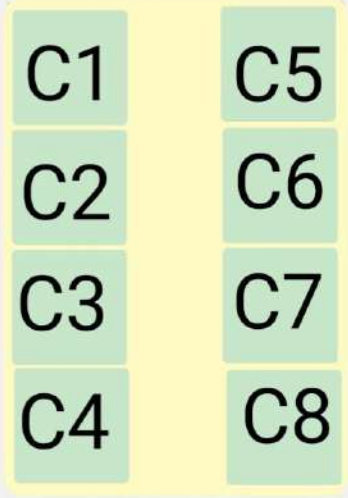
plastic card layer

ARCHITECTURE OF SMART CARD



ELECTRICAL CONTACT OF SMART CARD

position	abbrevation	function
C1	Vcc	Supply Voltage
C2	RST	Reset
C3	CLK	Clock Frequency
C4	RFU	Reserved for future use
C5	GND	Ground
C6	Vpp	External programming voltage
C7	I/O	Serial input/output communications
C8	RFU	Reserved for future use



WORKING OF SMART CARD

Smart card is inserted into the card reader which reads the information from the smart card.

After the card reader reads information from the card it passes the information to the payment system or authentication system.

There after the payment system or authentication system authenticated the user that whether the provided data matches with the database.

In last step the payment system or the authentication system does the required task

TYPES OF SMART CARD

- contact smart card
- contactless smart card
- dual interface card
- memory based smartcard
- micro processor based smart card
- hybrid smart card

SECURITY FEATURES

- Human-readable security features
- Security features of the smart card chip
- Security features of the operating system
- Security features of the network

HUMAN READABLE SECURITY FEATURE

- Photo lamination
- Signature strip
- Hologram
- micro printing
- embossing
- security pattern
- laser graver

SECURITY FEATURES OF SMART CARD CHIP

- Testing the microcircuit during the production
- it is converted to a mode Accessing the internal chip circuit is impossible for this mode
- To prevent attacks execution of some project is necessary
- The connections between on-chip elements are encrypted
- there are circuits in smart card which can detect external tampering.

SECURITY FEATURES OF CARD OPERATING SYSTEM

- Access to smart card files can be protected with a Personal Identification Number (PIN) or with cryptographic keys.
- PIN protected card access, with fine-grained access controls to data objects so that different areas of memory can be subject to different security rules
- When a pin isn't entered correctly then after number of attempts the smart card is deactivated

SECURITY FEATURES OF THE NETWORK

- design the transport protocol such that tampering will not affect the overall system security
- Some actions can physically secure the card termina
- placing the smart card reader and communications link in a secured environment can physically protect them.

SECURITY PRINCIPLE

- Privacy
- Non-repudiation
- Authentication
- Integrity
- Verification

Smart cards use different encryption algorithms to implement these principles.

PRIVACY

- The act of ensuring the nondisclosure of data between two parties from third party is privacy
- risk of privacy loss
- Symmetrical cryptography and asymmetrical cryptography are used to assure privacy
- implement of multiple algorithms is impossible Single standard algorithm will be used

NON REPUDIATION

- Non-repudiation confirms that the origin of data is exchanged in transaction
- A certain message that sent form a sender could never be denied by receiver
- Non-repudiation of the transaction is ensured by cryptography
- digital signature is an example

AUTHENTICATION

- Authentication is the process which specifying identity of person
- it specifies that someone or something is who or what it is claims to be
- Authority issuing the certificate guaranty certificates that the holder of certificate is who she/he pretends to be

INTEGRITY

- Cryptographic techniques confirm the correctness of message that transmitted from the original to the recipient this is known as data integrity
- Integrity assures that only those authorized can access or modify the information
- A data integrity service guarantees the correctness of content of message which we sent

VERIFICATION

- Confirming the identity of cardholder is the useful act before using a card
- Encryption technology is used to verify that another person is who to pretend to be
- pin code | biometrics | mutual verification

ATTACKS ON SMART CARD

There are three main types of attack that are considered in smart card security

- invasive attack
- semi invasive attack
- non invasive attack

INVASIVE ATTACK

- directly attacked through a physical means
- compromise the security of any secure microprocessor
- require very expensive equipment
- require large investment in time
- use of a focused ion beam to destroy or create tracks on the chips surface
- this attack is no longer possible

SEMI INVASIVE ATTACK

- require the surface of the chip to be exposed
- seeks to compromise the security of the secure microprocessor without directly modifying the chip
- injecting faults using laser light or white light

NON INVASIVE ATTACK

- seek to derive information without modifying a smart card
- both the secure microprocessor and the plastic card remain unaffected
- derive information by observing information that leaks during the computation of a given command
- attempt to inject faults using mechanisms other than light

COUNTERMEASURE FOR NON INVASIVE ATTACK

- constant execution
- Random delays
- Randomisation
- randomized execution

The above list gives the countermeasures that would need to be applied to a cryptographic algorithm to render it secure against side channel analysis

FAULT INJECTION MECHANISM

- variation in supply voltage
- variation in the external clock
- extremes of temperature
- laser light
- white light
- electromagnetic flux

COUNTERMEASURE FOR FAULT INJECTED MECHANISM

- checksums
- execution randomisation
- random delays
- execution redandancy
- variable redundancy
- rectification counters and baits

ADVANTAGES

- more secure
- prevents fraud
- offer a variety of benefits
- safe to transport
- time saving
- double as an id card
- less expensive

APPLICATIONS

- domestic
- secured physical access
- government application
- banking application
- e-commerce and retail
- telecommunication

DISADVANTAGES

Possible Risk of Identify Theft:-
Smart cards are vulnerable to hardware hacking which means that data stored in the card can be altered or corrupted

Slow Adoption:-
If used as a payment card, not every store or restaurant will have the hardware necessary to use these card

DISADVANTAGES

Easily Lost:-
Smart cards are small, lightweight and can be easily lost if the person is irresponsible Since smart cards have multiple uses the loss may be much more inconvenient

Security:-
Another drawback of using smart cards is their level of security. They are more secure than swipe cards.

CONCLUSION

The major highlight of the smart card technology is the security it affords users. With the smart card, users can store personal information like bank records, student identity to access exclusive libraries, company identity cards to gain access through computerized security checkpoints, storing phone contacts as in sim cards and many other huge benefits that guarantee the security of personal data.

REFERENCE

- Elprocus Website
- Electricalfundablog Website
- International Journal of Security (IJS), Volume (5) : Issue (2)
  By Hamed Taherdoost, Shamsul Sahibuddin & Neda Jalaliyoon
- Smart Card Security
  By Michael Tunstall Keith Mayes Konstantinos Markantonakis
- smart card content security
  By Stefano Zanero

THANK YOU