Research Paper on Smart Cards

Pawan Kumar

Department of Computer Science, Stevens Institute of Technology

CPE 550-A, Computer Organization and Programming

Dr. Edward Banduk

November 30th, 2021

Smart Cards

1. Introduction to smart cards

A smart card, chip card, or integrated circuit card (ICC or IC card) is a physical electronic authorization device, used to control access to a resource. It is typically a plastic credit card-sized card with an embedded integrated circuit (IC) chip. Smart cards can provide personal identification, authentication, data storage, and application processing. Applications include identification, financial, mobile phones (SIM), public transit, computer security, schools, and healthcare. Smart cards may provide strong security authentication for single sign-on (SSO) within organizations. This research is chiefly to study the necessity of smart card in today's world and assess the security aspects effect on smart card technology adoption.

2. History of smart cards

The idea of incorporating an integrated circuit chip onto a plastic card was first introduced by two German engineers in the late 1960s, Helmut Gröttrup and Jürgen Dethloff. In 1968 and 1969 German electrical engineers Helmut Gröttrup and Jürgen Dethloff jointly filed patents for the automated chip card. In 1974 Roland Moreno, a French independent inventor, mounted a chip on a card and devised a system to use the card for payment transactions. He showed his invention to a few French banks, and by the end of the year Honeywell Bull had produced the first CP8 Transac cards. In 1977, Michel Ugon from Honeywell Bull invented the first microprocessor smart card with two chips: one microprocessor and one memory, and in 1978, he patented the self-programmable one-chip microcomputer (SPOM) that defines the necessary architecture to program the chip. The early adopters of the new card were both French: France Telecom and Carte Bancaire. The first company is the state-owned telecommunications monopoly, it decided to issue tamper-proof calling cards. The second is now the leading French credit card network, it began by using the CP8 Transac to issue VISA and MasterCard credit cards (the card still had a magnetic stripe in order to preserve international compatibility). In the European standard for digital mobile telephony GSM, a smart card is used as a form of identification of the user. A slot in all GSM telephones allows the user to be identified independently of the equipment. This means that a user could borrow a friend's phone after his had run out of credit, but still have the call billed to his, not his friend's account.

In the form of credit cards and SIM cards, smart cards are the most common form of IT processing power on the planet. It's is estimated that between 30 to 50Billion smart cards are in circulation today.

3. Design of smart cards

A smart card may have the following generic characteristics:

- Dimensions similar to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimetres (3.37 in × 2.13 in). Another popular size is ID-000, which is nominally 25 by 15 millimetres (0.98 in × 0.59 in) (commonly used in SIM cards). Both are 0.76 millimetres (0.030 in) thick.
- Contains a tamper-resistant security system (for example a secure crypto processor and a secure file system) and provides security services (e.g., protects in-memory information).
- Managed by an administration system, which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.
- Communicates with external services through card-reading devices, such as ticket readers, ATMs, DIP reader, etc.

- Smart cards are typically made of plastic, generally polyvinyl chloride, but sometimes polyethylene-terephthalate-based polyesters, acrylonitrile butadiene styrene or polycarbonate.

Since April 2009, a Japanese company has manufactured reusable financial smart cards made from paper.

4. Working of smart cards

Smart Card working process:

- Step-1: Smart card is inserted into the card reader which reads the information from the smart card.
- Step-2: After the card reader reads information from the card it passes the information to the payment system or authentication system.
- Step-3: There after the payment system or authentication system authenticated the user that whether the provided data matches with the database.
- Step-4: In last step the payment system or the authentication system does the required task.

5. Types of Smart Cards

a) Contact Smart Card:

This type of smart cards is embedded with electrical contacts which are used to connect to the card reader where the card is inserted. The electrical contacts are deployed on a conductive gold-plated coating on the card surface.

b) Contact less Smart Card:

This type of smart card establishes connection with the card reader without any physical contact. It consists of an antenna by means of which it is used to communicate using radio frequency band with the antenna on the reader. It receives power from the reader via the electromagnetic signal.

c) Dual-interface cards:

This type of smart card is equipped with both contact less and contact interfaces. This type of card enables secure access to the smart card's chip with either the contact less or contact smart card interfaces.

d) Memory based smart card:

This type of smart cards are embedded with memory circuits. It stores, reads and writes data to a particular location. It is straight memory card which is only used to store data or a protected memory card with a restricted access to the memory and which can be used to write data. It can also be a rechargeable or a disposable card which contains memory units which can be used only once.

e) Microprocessor based smart card:

This type of smart cards consist of microprocessor embedded onto the chip in addition to the memory blocks. It also consists of specific sections of files related with a particular function. It allows for data processing and manipulations and can be used for multi functioning.

f) Hybrid smart card:

Hybrid smart card embedded with both memory and microprocessor. Two different chips are used for different applications connected to a single smart card based on the different functionality as the proximity chip is used for physical access to prohibited areas while the contact smart card chip is used for sign in authentication.

6.) Applications of Smart Cards

a) Financial

Smart cards serve as credit or ATM cards, fuel cards, mobile phone SIMs, authorization cards for pay television, household utility pre-payment cards, high-security identification and access badges, and public transport and public phone payment cards. Smart cards may also be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters, vending machines or merchants.

b) SIM

The subscriber identity modules used in mobile-phone systems are reduced-size smart cards, using otherwise identical technologies.

c) Identification

Smart-cards can authenticate identity. Sometimes they employ a public key infrastructure (PKI). The card stores an encrypted digital certificate issued from the PKI provider along with other relevant information. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and other cards used by other governments for their citizens. If they include biometric identification data, cards can provide superior two- or three-factor authentication.

d) Public transit

Smart cards, used as transit passes, and integrated ticketing are used by many public transit operators. Card users may also make small purchases using the cards. Some operators offer points for usage, exchanged at retailers or for other benefits. Examples include Singapore's

CEPAS, Malaysia's Touch n Go, Ontario's Presto card, Hong Kong's Octopus card, London's Oyster card, Ireland's Leap card, Brussels' MoBIB, Québec's OPUS card, San Francisco's Clipper card, Auckland's AT Hop, Brisbane's go card, Perth's SmartRider, Sydney's Opal card and Victoria's myki.

e) Video games

In Japanese amusement arcades, contactless smart cards (usually referred to as "IC cards") are used by game manufacturers as a method for players to access in-game features (both online like Konami E-Amusement and Sega ALL.Net and offline) and as a memory support to save game progress. Depending on a case-by-case scenario, the machines can utilize a game-specific card or a "universal" one usable on multiple machines from the same manufacturer/publisher.

f) Computer security

Smart cards can be used as a security token. Mozilla's Firefox web browser can use smart cards to store certificates for use in secure web browsing. Some disk encryption systems, such as VeraCrypt and Microsoft's BitLocker, can use smart cards to securely hold encryption keys, and also to add another layer of encryption to critical parts of the secured disk.

7. 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 algorithm. There are, however, several methods for recovering some of the algorithm's internal state. Differential power analysis involves measuring the precise time and electric current required for certain encryption or decryption operations. This can deduce the on-chip private key used by public key algorithms such as RSA. Some implementations of symmetric ciphers can be vulnerable to timing or power attacks as well.

8. Benefits

Benefit #1: Persistent, protected storage

Persistent storage is one advantage of smart cards. How much memory a card has depends on the application, but 1 KB to 256 KB is typical. This is dramatically more than the approximately 150 bytes that can be stored on a magnetic stripe card. The increased capacity also accommodates encryption capabilities. Once information is stored on a smart card, it is difficult to erase, alter or delete -- whether intentionally or accidentally. What makes the card smart is that not only does the microprocessor store data, but it also has its own OS that can process data in real time.

Benefit #2: Processing power

As most smart cards have a small CPU, they are capable of more than parroting data stored in the card. For example, the CPU can protect the information by requiring the user to enter a PIN. One significant security benefit of smart cards is that the CPU can count -- the same cannot be said about magnetic stripe cards. For example, enter the smart card PIN wrong seven times and the CPU may refuse to let the user try again for a specified period, such as one hour or one day. In some applications, the CPU may wipe the stored information if the PIN is entered wrong too many times or force the user to call a customer support number to retrieve a special unlock code.

Benefit #3: Packaging

The third advantage of smart cards is the packaging. Smart cards are usually made of plastic -- apart from the embedded microprocessor -- which is inexpensive to produce. While they are not as cheap as credit cards to manufacture, in moderate quantities of 100, for example, smart cards will cost less than $10 each. Inexpensive smart card readers are also available for less than $50. This makes the smart card system dramatically less expensive than digital tokens and other authentication technologies.

9. Disadvantages

The plastic or paper 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 and antenna in contactless cards. PVC cards can crack or break if bent/flexed excessively. However, for large banking systems, failure-management costs can be more than offset by fraud reduction. The production, use and disposal of PVC plastic is known to be more harmful to the environment than other plastics.

10. Conclusion

Smart-cards now widely adopted in variety of industries for their ability to store and communicate a large amount of data in a secure device. Smart cards offer increase security, convenience, and economic advantages, due to which smart cards have become a necessity in today’s world.

References

1) Wikimedia Foundation. (2021, November 16). Smart card. Wikipedia. Retrieved November 17, 2021, from https://en.wikipedia.org/wiki/Smart_card.

2)Smart cards. (n.d.). Retrieved November 17, 2021, from http://web.mit.edu/ecom/Spring1997/gr12/0intro.htm.

3) Smart card basics – A short illustrated guide (June 2021). Thales Group. (n.d.). Retrieved November 17, 2021, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/smart-cards-basics.

4) Working and types of smart card. GeeksforGeeks. (2019, August 8). Retrieved November 17, 2021, from https://www.geeksforgeeks.org/working-and-types-of-smart-card/.