A Study of Smart Card and its Security Features

ECE 578 Computer and Network Security Project Report
Oregon State University

By
Nimmi Kalinati

Index

1. Introduction

What is a smart card ?

Smart card is an intelligent token that is identical in size and feel to a credit card with an integrated circuit chip located within its body. It provides not only memory capacity, but computational capability as well. The self-containment of smart card makes it resistant to attack, as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in different applications, which require strong security protection and authentication.

Where can it be used ?

Smart card can act as an identification card, which is used to prove the identity of the card holder. It also can be a medical card, which stores the medical history of a person. Furthermore, the smart card can be used as a credit/debit bank card which allows off-line transactions. All of these applications require sensitive data to be stored in the card, such as biometrics information of the card owner, personal medical history, and cryptographic keys for authentication, etc. New information and/or applications can be added depending on the chip capabilities.

What are the different types of smart cards ?

Contact Smart Cards are the ones that have to be inserted into a smart card reader. These cards have a contact plate on the face, which makes an electrical connector for reads and writes to and from the chip when inserted into the reader.

Contactless smart cards have an antenna coil, as well as chip embedded within the card. The internal antenna allows for communication and power with a receiving antenna at the transaction point to transfer information. Close proximity is required for such transactions, which can decrease the transaction time while increasing convenience.

A *combination card* functions as both contact and contactless smart card.

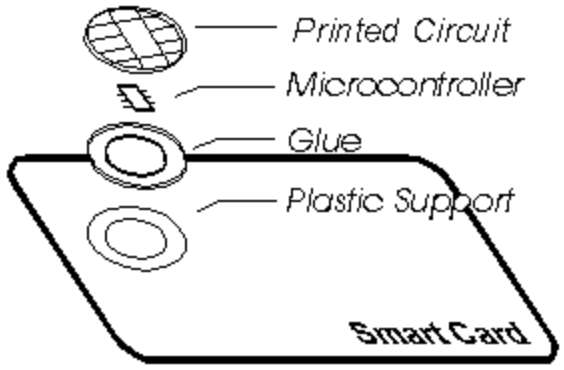
What are its benefits over magnetic stripe cards ?

The amount of information that can be stored on smart card is over a thousand times more than that of magnetic stripe card. In addition, smart cards are more reliable, perform multiple functions and are more secure because of high security mechanisms such as advanced encryption and biometrics. Another important benefit of smart card is that it is a renewable security element. If appropriately used, they can change their cryptographic keys and algorithms as required.

In the near future, the traditional magnetic strip card will be replaced and integrated together into a single card by using the multi-application smart card, which is known as an electronic purse or wallet in the smart card industry. The smart card is becoming more and more significant and will play an important role in our daily life. It will be used to carry a lot of sensitive and critical data about the consumers ever more than before when compared with the magnetic strip card. Therefore, there are many arguments and issues

about whether or not the smart card is secure and safe enough to store that information. This has always been a source of controversy.

2. Physical Design



The picture shown above models a smart card that was in use a few years back. Recent cards are of course more advanced. The printed circuit conforms to ISO standard 7816/3 which provides five connection points for power and data. It is hermetically fixed in the recess provided on the card and is burned onto the circuit chip, filled with a conductive material, and sealed with contacts protruding. The printed circuit protects the circuit chip from mechanical stress and static electricity. Communication with the chip is accomplished through contacts that overlay the printed circuit.

The capability of a smart card is defined by its integrated circuit chip. Typically, an integrated circuit chip consists of a microprocessor, read only memory (ROM), non static random access memory (RAM) and electrically erasable programmable read only memory (EEPROM) which will retain its state when the power is removed. The current circuit chip is made from silicon, which is not flexible and particularly easy to break. Therefore, in order to avoid breakage when the card is bent, the chip is restricted to only a few millimeters in size.

All the data exchanges are under the control of the central processing unit in the integrated circuit chip. Card commands and input data are sent to the chip which responses with status words and output data upon the receipt of these commands and data. Information is sent in half duplex mode, which means transmission of data is in one direction at a time. This protocol together with the restriction of the bit rate prevents massive data attack on the card.

In general, the size, the thickness and bend requirements for the smart card are designed to protect the card from being spoiled physically. However, this also limits the memory and processing resources that may be placed on the card. As a result, the smart card always has to incorporate with other external peripherals to operate. For example, it may require a device to provide and supply user input and output, time and date information,

power and so on. These limitations may degrade the security of the smart card in some circumstances as the external elements are untrusted and precarious.

3. Environment of a Smart Card Based System

Participants of the system

Card holder **:** This is the party who has day to day possession of the smart card. He may control the data on the card, depending on the system, but it is highly unlikely that he ad control of the protocols, software, or the hardware choices made in the creation of the card.

Data owner **:** This is the party who has control of the data within the card. In cases such as using the card as a mechanism for carrying digital certificates, the card owner is also the data owner. However, if the card is an electronic-cash card, the issuer of the cash is the data owner, and this split opens the possibility of attack.

Terminal : It is the device that offers the smart card its interactions with the world. The terminal controls all I/O to and from the smart card. If the card is used as a phone calling card, this is the pay phone owner. If the card is used as an ATM identification card, this is the ATM service provider.

Card issuer : This is the party who issued the card. This party controls the operating system running on the smart card, and any data that is initially stored on it. If the card is a telephone payment card, the issuer is the phone company. If the card is an employee ID card, the issuer is the employer. In some multi-function cards, the card issuer may have nothing to do with the applications running on the card, and may only control the operating system. In other multi-function cards, the same issuer may control all the applications running on the card.

Card manufacturer : This is the party that produces the smart card. Note that this is a simplification; the manufacturer may or may not own the fabrication facility in which the chips are actually made; they may have subcontracted design functions, and they may be using third party tools in their work, such as VHDL compilers. However, here all of these have been modeled as the card manufacturer.

Software manufacturer : This is the party that produces the software that resides in the smart card. This is again a simplification of a probably complex array of makers of compilers, utilities, etc.

Life Cycle

From the manufacturer to application provider, then the card holder, the production of a smart card is divided into different phases as discussed below.

Fabrication Phase

This phase is carried out by the chip manufacturers. The silicon integrated circuit chip is created and tested in this phase. A fabrication key (KF) is added to protect the chip from fraudulent modification until it is assembled into the plastic card support. The KF of each chip is unique and is derived from a master manufacturer key. Other fabrication data will be written to the circuit chip at the end of this phase. Then the chip is ready to deliver to the card manufacturer with the protection of the key KF.

Pre-personalization Phase

This phase is carried out by the card suppliers. In this phase, the chip will be mounted on the plastic card which may have the logo of the application provider printed on it. The connection between the chip and the printed circuit will be made, and the whole unit can be tested. For added security and to allow secure delivery of the card to the card issuer, the fabrication key will be replaced by a personalization key (KP). After that, a personalization lock V_{PER} will be written to prevent further modification of the KP. In addition, physical memory access instructions will be disabled. Access of the card can be done only by using logical memory addressing. This preserves the system and fabrication areas being accessed or modified.

Personalization Phase

This phase is conducted by the card issuers. It completes the creation of logical data structures. Data files contents and application data are written to the card. Information of card holder identity, PIN, and unblocking PIN will be stored as well. At the end, a utilization lock V_{UTIL} will be written to indicate the card is in the utilization phase.

Utilization Phase

This is the phase for the normal use of the card by the card holder. The application system, logical file access controls, and others are activated. Access of information on the card will be limited by the security policies set by the application. This will be discussed in detail in the next section.

Invalidation Phase

There are two ways to move the card into this phase. One is initiated by the application, which writes the invalidation lock to an individual file or the master file. All the operations including writing and updating will be disabled by the operating system. Only read instructions may remain active for analysis purposes. The other way to put the card into this phase is that, when the control system irreversibly blocks access because both the PIN and unblocking PIN are blocked, then all the operations will be blocked including reads.

Types of Attacks on a Smart Card Based System

Since a large number of parties are involved in any smart card based system, there are several types of attacks that have to be considered. Here we will look at the attacks by the system participants against one another.

Terminal Against the Cardholder or Data Owner

These are the easiest attacks to understand. When a cardholder puts his card into a terminal, he is trusting the terminal to relay any input and output from the card accurately. The ability for a rogue terminal to do damage in this environment is significant, and it is impossible for the cardholder to detect this kind of fraud in the context of a single terminal. Prevention mechanisms in most smart card systems center around the fact, that the terminal only has access to a card for a short period of time. Software on the card could limit the amount of damage a rogue terminal could do. However, there are prevention mechanisms that involve having the user own the smart card terminal, such as one attached to a personal computer. The real prevention mechanisms, though, have nothing to do with the smart card/terminal exchange; they are the back-end processing systems that monitor the cards and terminals, and flag suspicious behavior.

Cardholder Against the Issuer

Such attacks target the integrity and authenticity of data or programs stored on the card. These attacks are made possible by the issuer's decision to use a smart card system where the cardholder holds data for the issuer or other party. Using the pay telephone application as an example, if the phone were to use an account-based system, where a simple card holds a very long account number that is used by the phone company to dereference an account stored on a back-end system, then there are account guessing and theft attacks based on the numbers. This sort of system can be enhanced by adding a challenge/response or inverted hash chain mechanism for sending replay resistant passwords. If the card issuer chooses to put bits that authorize use of the system in the card, they should not be surprised when those bits are attacked. These bits could be authenticated account numbers, or it could be a system with a key buried within the card, on the assumption that this key cannot be extracted, and proper completion of the protocol indicates that the card has not been tampered with. These systems all rest on the questionable assumption that the security perimeter of a smart card is sufficient for their purposes.

Cardholder Against the Software Manufacturer

When the card is issued to an assumed hostile user, the assumption exists that the card will not have new software loaded onto it. This is enforced by the use of pre-issuance stages with various one-way transformations being employed by the card manufacturer to ensure that the software is not tampered with. The underlying assumption may be that the split between card owner and software owner is unassailable,

and relies on the separation being strong. However, attackers have shown a remarkable ability to get the appropriate hardware sent to them to aid in launching an attack.

Cardholder Against the Data Owner

Data stored on the card must be protected from the cardholder in many cases. In some cases, the cardholder is not allowed to know that data. A building access card, for example, could have a secret value inside the card; knowledge of this value could allow the cardholder to make additional access cards. In other cases, the cardholder is allowed to know the value, but not allowed to change it. If the card is a stored-value card, and the user can change the value, he can effectively mint money. There are two essential characteristics of these attacks. One, the card must act as a secure perimeter, preventing the cardholder from accessing the data inside the card. In this context, the card may need to be fairly confident that it will detect and respond to attacks with a minimum of control over its environment. And two, the attacker has access to the card on his own terms. He is allowed to take the card into his laboratory and perform whatever experiments he wants in order to learn how they work. There have been many successful attacks against the data inside a card. These attacks include reverse-engineering and defeating tamper resistance, fault analysis, and side channel attacks such as power and timing analysis.

Issuer Against the Card Owner

Most systems assume that the card issuer holds the best interests of the cardholder. This is not necessarily the case, and a malicious issuer can launch several attacks against cardholders. These attacks are typically privacy invasions of one kind or another. Smart card systems that serve as a substitute for cash must be designed very carefully to maintain the anonymity and unlinkability that are a property of cash money. Attacks or design failures can substantially reduce the privacy of the system. Alternately, a system may be sold as having more privacy than it in fact offers, allowing the issuer to gather data surreptitiously about the cardholders. Features introduced into the card as the system matures may alter initial characteristics of the system with substantial impact on the privacy of the system. This can count as an attack by the issuer because the cardholder is rarely asked or able to discern the security impact of a change to the system made by the issuer. These changes are often not optional from the customer's viewpoint; the only choices are to accept the upgrade or leave the system. Lastly, this type of attack may be carried out by the issuer, or by the hardware or software designer, in collaboration with terminals, without the knowledge or consent of the issuer.

Cardholder Against the Terminal

These attacks are very subtle. These involve fake or modified cards running rogue software, with the intent of subverting the protocol between the card and the terminal. Good protocol design mitigates the risk of these kinds of attacks, which can be made more difficult by hard-to-forge physical aspects of the card (e.g., the hologram on Visa and MasterCard cards), which can be checked by the terminal owner manually. Note

that digital signatures on the software are not effective here since a rogue card can always lie about its signature, and there is no way for the terminal to peer inside the card. Defending against this kind of attack requires another function split: the cardholder must not be able to manipulate the data inside the card.

Manufacturer Against the Data Owner

Sometimes, a few designs by manufacturers may have substantial and detrimental effects on the data owners in a system. By providing an operating system that allows or even encourages multiple users to run programs on the same card, a number of new security issues are opened up. The first, and most obvious, is subversion of the operating system and subsequently other programs. Even if the smart card operating system can be made secure, issues of user interface security remain and are exacerbated by the smart card's handicaps. How is the user to know what program is running when the card is inserted into a terminal? How to ensure that your program is talking to the terminal, and not through another program? How can a program that believes itself compromised terminate safely, and signal outward the cause for its demise? Or should it even try; what interesting attacks might become possible if a card announces its own imminent suicide? Can the card ensure that once such a message is sent the action of destroying its memory is completed, in the presence of a possibly hostile power supply? Less obvious would be intentionally poor random number generators, or other aspects of cryptographic implementation that are difficult and arcane areas to. The manufacturer is in an admirable position to engage in kleptographic attacks. Of the major smart card vendors, none has an admirable record of creating operating systems that were free of exploitable vulnerabilities. In addition, by providing implementations of various supporting protocols, the vendor may be in a position to leak an application's keys using any of several subliminal channels. And finally, it is possible for one application on a smart card to subvert another application running on the same smart card. It has been shown how to take a secure protocol and to create another protocol, also secure, such that the second protocol breaks the first protocol if both are running on the same device using the same keys.

Terminal Owner Against the Issuer

In a pre-paid phone card system, the terminal controls all communication between the card and the card issuer (generally the back-end of the system). In this system, the terminal can always falsify records that have nothing to do with the smart card, refuse to record transactions, etc. The terminal can also fail to complete one or more steps of a transaction to facilitate fraud or create customer service difficulties for the issuer. By failing to complete the action of debiting a card, a terminal can cheat the issuer, or by completing a transaction and not offering service (i.e., a pay phone) can create a service nightmare. These attacks are not related to the smart card nature of the system, and are simply attacks against the relationship between the terminal owner and the card issuer. Some systems try to mitigate this threat by having the card and back-end computer make a secure connection through the terminal. Many systems use monitoring on the back end to reduce the effectiveness of these attacks.

Impersonation Attack

These attacks are based on changing the roles played by various parties. The essential character of such an attack is that a party is transformed, leading to an unexpected set of motivations for that party. When a card is stolen, the new cardholder has lost all interest in maintaining the security of the account, and possibly in the physical integrity of the card. Thus, when a system assumes that the data stored on a card is secure because the interests of the cardholder and issuer are aligned, a vulnerability is opened by the theft of the card. Monitoring attacks can attack the privacy of the transactions made by the card or the secrecy of PIN or other data. The latter is probably a precursor to an active attack, not necessarily in the domain of the smart card protocol.

Third Party Attacks Using Stolen Cards

The difference between this attack and an attack by the cardholder is that, the thief does not have access to any secret information required to activate the card and the thief has only a limited amount of time to carry out his attack before the cardholder will notice that his card has been stolen. Hence, all the attacks by the cardholder are possible with the following addition: the thief is not concerned with any long-term repercussions against the legitimate cardholder. It is possible to build defenses into the system either at the card's or at the issuer's level. At the card level, there are perimeter and anomaly defenses available. The perimeter defense is that the card can consider several bad PIN attempts to be indicative of attack. The anomaly detection defense would be for the card to store history information and detect a pattern change in its use. This is an aggressive requirement, but in those cases where a card can be used offline, it may make sense to raise a flag of some type, possibly requiring contact with its issuer before additional use to allow the back end system a chance to make a more elaborate or sophisticated decision, or perhaps simply to defend the system against card duplication.

Measures to Counter the Attacks

Since smart cards are tamper resistant and not tamper proof, while implementing any system that uses them, the designer must ensure that every link in the security chain is secure enough when comparing to the risks of compromise versus the costs to secure.

There are three steps for implementing security in smart cards. They are *prevention*, *detection* and *response*.

Prevention

The first step in the design is to review the security of every link in the security chain. It is vital to that no weak link exists, as this will be the likely point of attack. One of the most common oversights is to assume the people working with the system aren't

vulnerable to various temptation or threats. A designer that overlooks this puts the system and individuals at risk. Potential attackers typically look for the greatest return on their investment, so a security designer should ensure that every element of the system is secure enough to deflect potential attackers to a more rewarding target.

Detection

The second step is to design in methods of detection. One must assume every element is a possible target. Just as banks have panic buttons for the tellers and perimeter security alarms, so should systems, which use smart card technology. Methods to detect, measure and isolate fraudulent activity are vital to the security management. Credit Card systems tolerate a certain amount of fraudulent activity, but is measurable and considered a part of doing business.

Response

Countermeasures are the third step in the design. Once the level of fraudulent activity justifies a response, then appropriate measures are taken. This is where the detection and isolation are important. It allows security managers to implement appropriate responses. For instances, it may be less expensive to have local law enforcement investigate than to upgrade system software or hardware.

On a different note, each time a system has the design role of two or more parties merged into one, the avenues of attack that are available to one of those parties against the other disappears. Contrariwise, ***adding parties to the system opens new venues of attack***, which need to be considered. The separation of the terminal and card from each other creates a venue, which could scarcely have been designed better to enable man-in-the-middle attacks. Considering the smart card's inability to communicate with the outside world, the simplest split reduction is to ensure that the cardholder and data owner are one. This will eliminate attacks by the cardholder on the data that currently plague most existing systems.
Also, it is widely understood by the security community that the ***best way to ensure the security of a system is to allow widespread public examination of it***. It has been shown repeatedly that interested attackers will obtain specifications or attack the system without them, and that open publication leads to review and analysis. Combining the mechanisms of simplicity and openness greatly simplifies the task of reviewers who choose to examine a system. Thus, reducing the number of parties not only eliminates entire classes of attacks as shown above, but it also makes the task of analyzing the system simpler. The simplicity of the security analysis will likely cause the analysis to occur sooner, as well as giving it a higher likelihood of success.

But an important benefit of smart card technology is that they are a renewable security element. If appropriately used, they can change their cryptographic keys and/or algorithms as required. Another point to remember is that smart cards typically carry some company logo or brand and for marketing reasons, they are replaced every 2 to 3 years. During this renewal process, new countermeasures can be designed in.

A last point to consider is that security is a never-ending battle. As technology improves, both sides of the battle have better tools to work with. Smart Card manufacturers invest millions of dollars on improving the security and they leverage the millions invested by the silicon providers.

Conclusion

This is still an evolving technology. But due to the several advantages that it offers, it is gaining popularity among users. This technology lacks any kind of man-machine interface, but relies on the card accepting host to provide such interface, thus allowing it to be customized according to the application domain. Using it provides security services in the information highway environment, bringing individualized security, moving away from the terminals towards individual users and low cost security, making it affordable to consumer applications along with the ease to use feature.

This report was written in an attempt to study the smart card system, and analyze its security features, various kinds of attacks that it is susceptible to and measures to counter such attacks.

References

1. An Overview of Smart Card Security, by CHAN, Siu-cheung Charles. http://home.hkstar.com/~alanchan/papers/smartCardSecurity

2. Which Smart Card Technologies will you need to ride the Information Highway safely ? , by Patrice PEYRET

3. Security and Smart Card, by Charles Cagliostro. http://www.scia.org/knowledgebase/aboutSmartCards/security.html

4. Smart Cards, Seizing Strategic Business Opportunities, by Catherine A. Allen and William J, Barr

5. Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards, by Bruce Schneier and Adam Shostack.