IDENTIFYING THREATS TO TRUST RELATIONSHIPS IN IC CARD-BASED SYSTEMS

Teddy Hsu
Information Security Group,
Royal Holloway, University of London
Surrey TW20 0EX, UK
C.HSU@rhul.ac.uk, Tel: +441784 466531

June 12, 2003

Abstract

Devices with integrated circuit chip are often seen as portable miniature PC with storage and processing capabilities. However, there are fundamental differences between a smart card and a conventional desktop PC or notebook in terms of the processor, input/out methods, and communication protocols. The differences become more obvious as a smart card is often operated in multiple environments, where not all devices are regarded as trusted parties.

In this paper we tend to identify potential threats to smart card-based systems emerged from possible trust breaches among communication participants in an environment in which a smart card is operated. Possible countermeasures will be discussed at the end of the paper.

Keyword: Smart Card, Trust Breaches, Trust Environment, Communication Participants, Attack Variations, Countermeasure Models.

1 Introduction

Strong security features of smart cards are being described as one of the major advantages of any chipcard-based technology in use today. Chip-based cards are seen as the most secure, durable, and portable data storage and processing devices. Nevertheless, few have actually looked into the potential breaches in the trust environment in which such device is operated, and the protocols used for information exchange. Security problems are commonly triggered by breaches in trust between the communicating entities. Therefore it is important to determine how trust breaches will lead to security problems in a smart card system.

It is generally accepted that it could be much harder to break a smart card's security than hacking into a normal PC or a notebook. And due to its processing and storage capabilities, those devices are sometimes also nick-named "Miniature PCs". Nevertheless, we must understand that there are fundamental differences between a PC with a hard disk, and a chip-based device in terms of access method, data input/output, and protocols used for communication with the outside world. Understanding the strength of a particular system requires an in-depth analysis of every components involved in such system in order to determine potential threats and resistance models. In this paper discussions are concentrated on how trust could be broken by different entities.

1.1 IC Devices and PC

The most important aspect of any smart card system lies in the protocols used for information and data exchange, in which they differ from a conventional PC. The components that make up a general PC consist of a CPU, hard disk, I/O devices, and power supply. the CPU is the core of a PC, responsible for computation and is conveniently joined with the disk drives, memory, and general I/O devices.

Now considering a smart card, which itself does not have any means of I/O device, a user must input information through a keypad attached to a terminal. In a hostile environment, information entered can be recorded or intercepted. The attacker can later analyse the information to perform cloning attacks. There may be lines attached to the reader that send information to other devices (the attacker's monitor or printer) of which the user is unaware. The information is displayed on the screen, which the user has no choice but to trust. There are many other differences but the fundamental one is restricted in the I/O devices. In the traditional PC, the user can modify the files and applications stored on the computer. But in the case of a multi-application smart card system, the cardholder, or even

the issuer, may not possess any ability to control the software running on the card. The characteristics and functionality of a smart card system are separated in a way that is different from a conventional computer.

2 Identifying Participants in a Smart Card System Trust Boundary

It is necessary to understand what parties are involved in a smart card-based system. This modelling process is quite important in understanding the system, as components in such a system often belong to different parties. In a typical chip card-based system, the following parties are constantly present:

- **Smart Card** - A Smart Card is a credit-card sizes card made of plastic with an embedded ICC (integrated circuit chip). The capabilities of a smart card lies in its CPU and micro-controller which enable the card to perform authentication and cryptographic algorithms. Data and files can be accessed and processed on-board, therefore there is no need for the secret information to leave the card. Smart card represents a unit which is used to store and process information in a smart card system environment.
- **Cardholder** - The cardholder is the party who has physical possession of the smart card, and has the day to day ability to use the card in various activities i.e. commercial transactions and network authentication. In most cases, this entity holds little influence in choosing as which components his card will be interacting with. For example, the control of the software application, hardware connectivity, and communication protocols.
- **Data Owner** - The data owner is the entity who owns the data stored on the smart card.
- **Terminal** - A Terminal represents means for a smart card to interact with the outside world. Smart card readers and other chip-reading devices are all kind of terminals, for example they are located at the POS (Point-of-Sale) to perform commercial transactions. The terminal allows all kinds of I/O (i.e. through keyboard and screen) to and from the smart card.
- **Card Manufacturer** - This party is responsible for manufacturing and supplying the physical smart card to the card issuer.
- **Chip Manufacturer** - They manufacturers the integrated circuit chips and supplies to the card manufacturers. Card manufacturers may not have the

facilities to produce the chip themselves, therefore subcontracting chip fabrication to different chip manufacturers, who may use different design tools. Here we can see a simple issue of trust between the subcontractors and the card manufacturers, and opportunities to subvert manufacture of the smart card can rise at this point.

- **Application Supplier** - They typically design applications targeted at a specific smart card operating system, then negotiate with the card issuer to download its application to be used with the card. Once again the issue of trust arises from suppliers using different compilers and tools to produce software packages.

- **Card Operator** - It is a unique authority whose role could be played by either the application provider or the card issuer. They interact with the smart card, either to perform some administrative tasks[1] or to run an application, or both. In most cases, both the card issuer and the software provider will play more or less the role of card operator.

3 Understanding the Causes of Trust Breach

3.1 Multi-purpose Smart Card

Although smart card possesses the ability to run multiple applications, however, most cards in use today are still designed to serve just one purpose. For example, a stored-value phonecard and digital ID cards for access control. In a single-purpose card system, the application, data, and the card belong to the card issuer, in which case the management of data, application, and memory space is simple. Such management approach becomes inadequate if more than one applications are used. Many other issues will need to be taken into account, such as memory partition, access privilege, data sharing rights, and file logical structure etc. The design of each element would affect the system's infrastructure and its operability. On a multi-application smart card, there is an operating system used to manage the card resources (such as memory, files, cryptographic engine etc) and applications. The resources stored on the card can come from various sources. Take Java Card for example, its security features against malicious codes have been widely discussed, however, not all smart cards use Java technology, and there still lacks a widely recognised policy for multi-application smart cards.

Multi-application smart card are getting more attentions and few obvious reasons are listed here: Reduced Number of Cards being Carried, Easy Post-Issuance

Updating (hence Reduced Time for Card Issuer to Release New Products to the Market), and Possible Synergies Between Companies.

3.2 An Example of Breach of Trust

A smart card very much depends on external devices when it comes to establishing communications with other devices. For example, a card reader (here the card reader represents the smart card's I/O device) must be present for a smart card to send and receive data to and from a server. The potential problem here is that, the card reader could be an untrusted medium. Under such circumstances a smart card has become a handicapped device, as itself alone will not be able to communicate with the server without the external device. Unlike a desktop PC which usually operates in a single trusted environment, a smart card is usually being carried around and used in different locations. So it cannot be guaranteed that all the participating devices are trusted. Even a terminal is supplied and installed by a delegated supplier, however, they might not all comply to the security policies set by other parties (e.g. card issuer).
The situation becomes more complicated in a system in which the physical card, data, applications, and the card issuer belong to different parties. Moreover, to achieve maximum utilisation of the smart card capabilities, certain data sharing must be allowed. That said, each party engaged in such a system would not always be willing to reveal all the information to another entity. For example, the card issuer would not want the card holder to be able to modify the data stored on the card. Synergies among different participants cannot be easily achieved. We call this situation potential trust breaches in the smart card-based systems.

3.3 Understanding the Role

A complex array of parties controlling different elements can be seen in such a system. We now look at examples of applications of smart card and identify which party controls what in such a system. We will demonstrate how this situation may cause problems.

- **Access Card/Token** - In this application the card stores some kind of digital ID (e.g. username/PW, certificate etc) which is used to identify the token possessor in an authentication protocol. In a simplified case when the card is solely used for authentication, the card issuer, terminal provider, and even the data owner will be the company, and the cardholder will be the employee. In this case, we shall not worry about the trust splits since

most elements belong to one entity. The possibilities for attacks here are for the cardholder (hence the malicious employee) to attack against data and terminal. Nevertheless, in the case of multi-purpose access token (such as one used for both micropayment and access control), the terminal owner (e.g.vending machine supplier) might change to a third party who is not under supervision of the company's security control. This would lead to other classes of attacks on the smart card system.

- **Digital Identification Card** - Such device is used for storing various types of digital identifications such as username and password, biometric information, digital certificates, and other authentication credentials. In this application, we may assume that the card issuer will be the Certificate Authority (CA) who issues the cardholder a set of authentication credentials. The cardholder can also be the data owner, but the application owner and the terminal owner could be different parties.

- **Multi-Application Smart Card** - This is the most complicated application in which a smart card is used. In such system, the card manufacturer, chip manufacturer, software supplier, card issuer can all be, or supplied by, different parties. Terminals can be supplied by one of the participants above, or from another third party. There can also be multiple terminal owners, depends how many applications will be used on the card. The cardholder may own or have control on some of the data stored on the card, but other data can be owned by other entities. A simple example of a multi-application smart card system can be a credit card which is issued by a bank, but is also loaded with a loyalty programme which might be supplied by a airline company or a petrol station. In this case, the card is being used as an electronic purse for payment facilities, but is also a card that collects information and stores loyalty points for another company. Here we can obvious see the problem of who controls what data, and what information can be shared among the participants while others must remain secret to its rightful owner. In this situation, attacks can be carried out by any participant involved in this system.

The list above just includes some popular applications of smart card in use today. Separation of management in smart card applications can be found in many ways, and breaches in trust relationships are likely to occur under such circumstance.

4 Attacks Related to Breaches of Trust

4.1 Attacks - The Theory

Some attacks on smart cards are identical to those used to attack conventional computer systems, while others are being developed only to attack smart cards. A breach of trust can simply be defined as one or more parties involved in a smart card system, whose attempt is to cheat and falsify transaction information. We can generally categorise the attacks into invasive and non-invasive attacks. Invasive attacks on smart cards used to mean spending extensive amount of time and resources to probe into the hardware of smart card. The dividing factor between these two attack methods is the amount of time available and whether the physical characteristics of the card would be damaged or not. It is often the case that the purpose of carrying out an invasive attack is to eventually produce a result which can be used for more repeatable non-invasive attacks later. Attacks carried out by the system participants are common. For example, a cardholder may attempt to cheat on the terminal; the terminal owner may try to copy the data stored on the card, a card issuer tries to gather information from the cardholder in a non-legitimate way etc. Attacks carried out by an outsider means that he may use a stolen card to perform a transaction, and this means that the attacker temporarily becomes the cardholder and cheats on the terminal and other parties.

4.2 Modelling the Attacks

We now model some examples of attacks that could occur in smart card systems. We categorise attack classes by identifying the participants, discussing the splits in their roles in the protocols, and how they might lead to breaches in trust relationships in such a system.

4.2.1 Cardholder Attacks

Attacks in this category can be carried out by either the legitimate cardholder or by someone who has temporary possession of a stolen card. Here we will list a few examples.

- Cardholder Attacking Data and Data Owner - Any data stored on a smart card must be carefully protected by suitable mechanisms. Sometimes it may be necessary to prevent cardholder from being able to view other secret information stored on the card apart from his personal details. This is

to prevent the cardholder from being able to modify the data. For example, if the cardholder is given a secret value(which should only be known to the authentication server and the smart card) used for accessing building and networks , he might be able to duplicate the card. Some systems allow the cardholder to read the value of stored data (such as in a pre-paid phonecard system), while others have stricter protocols on accessing data by the cardholder. In most cases, cardholder is only allowed to know the value of the data, but not given the privilege to be able to modify it.

One important aspect here is to know that the cardholder, especially if he is the legitimate holder, will have access to the card on his own terms and time basis. He can take as long as it is worth to analyse the security of the card, then to perform possible attacks on it. He can even destroy the card in order to learn how it works, because he will be issued a new one free of charge from the issuer. Therefore the smart card itself must be designed as a secure perimeter, and any suspicious behaviours must be detected to prevent further analysis on the card data. There are many well-known attacks that can be carried out by the cardholder against data stored on the card, for example, the hardwiring attacks which includes microprobing, reverse engineering, fault generation and analysis etc[2]. These attacks usually require highly specialised technique and proper equipment. Nevertheless, a new method of attack[1] could mean that hardware attacks on smart card can be much cheaper and easier than previously done.

- Cardholder Attacking Terminal - This attack involves using fake or modified card in an attempt to cheat on the interactive device in the system. The purpose is to subvert the protocol between the card and the terminal. The security needed to fight this kind of attack should not rely only on protocol designs, but also education to the terminal operators to comply to agreed security checks. Embedding physical characteristics (e.g. hologram) onto the card can also be a good idea. These features will need to be checked by the terminal owner carefully while accepting cards.

- Cardholder Attacking Card Issuer - These attacks are mainly done for financial rewards. Although we say it is the cardholder attacking the card issuer, however, it is more likely that the cardholder is also attacking the programmes or the data stored on the card. The cardholder can also attempt to supply false information to the card issuer during the card application period. This kind of attack happens most often where the policy allows the cardholder to view/control the data. Card issuers often assume that a smart

[1] see Optical Fault Induction Attacks,Sergei Skorobogatov and Ross Anderson, May 2002

card itself is good enough to secure data and applications, therefore overlooks other important aspects in designing secure communication protocols in the system.

- Cardholder Attacking Application - This attack means a hostile cardholder tries to temper with the software installed on the smart card. During a smart card life cycle from the chip manufacturer to the card issuer, each party has some kind of authorisation schemes to prevent other parties launching malicious attacks on the card during its transit period. A software manufacturer should be authorised by the card issuer to install/remove programmes on the card. This protocol requires function split between the card issuer, software manufacturer, and the cardholder. Nevertheless, card issuers and software suppliers can do little to prevent cardholders from attacking what is already installed on the card.

4.2.2 Card Issuer Attacks

Card issuers are often regarded as the genuine party in such a system. Nevertheless the card issuer can launch attacks against other parties too. Card issuer's attacks may not be directly associated with financial rewards, but to discover cardholders' behaviour, or other data initially not given to them. Data could also be sold to a third party. In addition, privacy regulations are not the same throughout the globe, therefore an inferior system with poor protocol design may substantially reduce the ability for a cardholder to be anonymous in an transaction.

4.2.3 Terminal Owner Attacks

The terminal provides means for input and output functions to a smart card. When terminals are not supplied by a card issuig organisation, this introduces many kinds of possibilities for attacks. Data transmission between the card, terminal and back-end system may be intercepted, and although the information can be encrypted by the smart card, an attacker may still find other ways to analyse such information. The terminal may also display false information. There have been cases where fake ATMs were setup around town centre, tricking innocent cardholders to insert card and enter their PINs to withdraw cash. Other ways of malicious terminal owners attacks are still being discovered as technology advances. For example, a terminal may try to subvert or fail to complete one or more steps in a transaction protocol, leading the system to record falsified information or nothing at all. An power analyser may also be attached to the terminal without the cardholder's awareness, so during an transaction the power analyser would send

and receive disruptive signals in an attempt to alter the transaction data or analyse the power input/output. Because a smart card itself has limited processing capabilities, therefore more responsibilities should be given to the back-end system to monitor suspicious behaviour. For users to have their own smart card terminals would be a great advantage in combating such attacks (e.g. PC with integrated readers).

4.2.4 Software Manufacturers Attacks

Different software manufacturers design different security features, and the quality and design principles may vary too. Wrongly designed programme may affect the smart card system security, not to mention if it comes from a malicious attacker. The case becomes more complicated in a multi-application smart card system as different applications are installed onto a single card. By enabling a card to run multiple applications and also to share information would open up new issues to system security. The operating system of a smart card is its core element, as it is in charge of major operations inside the chip. Therefore poor operating system design would significantly submerge the security of the smart card system as a whole. In early days, the issuers had to commit to a specific application developer, operating system and chip for each service the issuer wished to provide to its customer. This leaves almost no flexibility to change any of these components without having to modify the whole system. Today there have been developments towards open operating systems that support multiple applications. Moreover, it is suggested that smart card operating system should be made relatively simple, hence any faults could be quickly detected and fixed before damage can take place[3]. The problem here is how fast they can react to a faulty situation and how they are going to retract millions of cards already issued. It is also hard to ensure that one application is as secure as another, and information may leak out through one or other channels. It is also possible that communication protocols used after the initial secure protocol would affect the system security.

4.2.5 Other Models

Different parties hold different interests in obtaining and maintaining the security of a smart card system. When their roles are replaced by an attacker, the interests in sustaining security is ignored. For example, a legitimate terminal owner's interest in system security is to facilitate the communication between the smart card and the a bank. If an attacker becomes the terminal owner, the terminal is now used for subverting the security of the system. Sometimes an attacker's intentions are not related to stealing information or gaining financial rewards, but simply to

have fun. For example, an attacker can enter wrong PINs several times just to block the card for its use, and this could be carried out by a malicious terminal to drive this attack. In fact, attacks from the legitimate cardholder and the attacker using a stolen card may be carried out in different manners. It is due to the information and time available to an attacker, and the amount of resources he has to carry out an attack. The above attacks could be prevented by designing a secure protocol that detects abnormal wrong PINs being entered, which can be indicative to a potential attack. The card should also have some level of record about pattern changes in the card usage, this will help detecting suspicious behaviour. Sometimes different parties would collaborate in order to carry out an attack more successfully. The main purposes would be to be able to obtain unauthorised services and information. The possibilities of collaborative attacks may grow as the number of parties increase in a smart card system.

5 Countermeasures

We have mentioned that the biggest problem in a smart card system is the separations in roles and responsibilities that lead to breaches in trust. Therefore the easiest way to improve security of a smart card system is to reduce the number of parties involved in the communication. However, this proposal is against the current trend in the smart card industry as companies are promoting the use of multi-application smart cards. Deploying a multi-application smart card often means increase in the number of parties in a system, because currently not all companies have the capabilities nor the resources to design and market everything needed to implement a complete smart card system. If it is possible to combine two or more roles in a multi-application smart card system, then many of the above mentioned attacks would simply disappear. Of course it is also possible to design more secure cryptographic protocols or defensive hardware and software mechanisms.

5.1 Reducing Number of Parties

We may say that the possibility of new attacks will increase when a new party joins the system. This is caused by splits in each party's interests and difference in their responsibilities. For many current systems it may be possible to combine the cardholder and data owner into one entity (or at least give certain control over some data to the cardholder), hence to eliminate the attacks from cardholder against data and data owner. Attacks carried out by terminal owners against cardholders and card data are more problematic to solve due to the physical characteristics of the

smart card. In order to keep a smart card's mobility, it is hard to add more hardware functionality to a chip such as a screen or a keypad. However, a portable keypad maybe be designed to be connected with the terminal and anything that comes out from the keypad (such as PIN) should be encrypted. This way the cardholder does not need to use the terminal's keypad which may have other devices intercepting secret information.

5.2 Secure System and Protocol Design

Strong security must be the guiding principle of the development of a system. Adding security features after a system has been implemented would most likely be a harder and expensive task, because it might involve a redesign of the whole system, its operations, management responsibilities and so on. This task would always be prone to mistakes because the modification might not be done by the same people who designed the system in the first place. Many organisations use single application smart card mostly because it offers more storage and can process simple information. They rely on the card itself to protect information while paying much less attention to their system and communication security. A system is as secure as its weakest link, therefore if an attacker can find a way to sneak into the back system he would not need to break a smart card's security feature. Security must be considered from the very beginning of a system design, and be coupled with ongoing reviews. This would not be a simple task as designing a secure system would involve considerations in a system's feasibility, measurability, logical review, user review, development review, and so on. The best way is to create a more open perimeters that will add transparency to both the design and operational stages of a system. We can also implement an authentication protocol for the card to be able to authenticate the terminal as a genuine terminal.

5.3 User Education

Education should be provided to the cardholder, terminal owner, and terminal operator. Often a simple skip in one step in a protocol could lead to breaches in system security. For example, using the magnetic stripe reader instead of the chip card slot. It is common that many terminal operators do not check a card's physical security adequately (e.g. signature). This greatly increases the chance of an attacker using a stolen card without being noticed. Education to users should involve detailed explanation of the card security features, system and protocol design, and terminal operations.

6 Conclusion

In this paper we have discussed different issues regarding smart card system security and we should understand now that it is very hard to find a complete solution to solve the problems. Function splits may be required for stronger protocol designs, but it might also create opportunities for breach of trust. There are technical difficulties and market preference issues to bring improvements to a smart card's physical and logical security attributes therefore it is wiser to design a system that has appropriate resistance mechanisms. We have also differentiated smart cards and traditional PCs in the beginning of this paper which should give a good insight into a good modelling and evaluating process of a system. Nevertheless, security is still largely down to the users who uses it as a convenient device because no matter how well-built the card and the system's security are, if the user chooses to ignore the protocols then the door for an attacker will be wide open.

References

[1] Pierre Girard. Which security policy for multiapplication smart cards? In *Proceedings of the 1st Workshop on Smartcard Technology*, Gemenos CEDEX - France, 1999. USENIX. Available from http://www.usenix.org.

[2] Lauri Karppinen. Attacks related to the smart card used un electronic payment and cash cards. In *Proceedings of the Helsinki University of Technology*, Laboratory of Telecommunications Software and Multimedia,Helsinki University of Technology, 2000. Available from http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers/.

[3] Konstantinos Markantonakis. An overview of multi-application smart card platforms, March 2002. Information Security Group RHUL Seminar Note, http://www.isg.rhul.ac.uk/ costasm.