Smart Cards

by Mahadev Karadigudda
Department of Computer Science, San Jose State University
mahadevk@yahoo.com

Abstract: Smart cards have been very popular as hardware tokens. Smart cards were invented with the idea of providing security. However, today, smart cards are of a variety of type, from behaving as simple storage devices to significantly computational devices. In this paper, we will introduce smart cards and look into ways in which smart cards assist in improving computer security. We also study and present a number of methods in which smart card security loopholes can be attacked.

Introduction: Smart card is a credit card sized plastic card with a chip embedded on it. ISO uses the term Integrated Circuit Card(ICC)[6] to cover all the devices that are used as identification plastic cards. Smart cards were first invented in 1968, by German inventors Jurgen Dethloff and Helmut Grotrup. However, later it was known that there were several other researchers in Japan and France who were also working on similar ideas, at around the same time. Initially, smart cards were deployed as prepaid phone cards. The success of these in preventing tampering, increased their acceptance and popularity.

Smart cards can be divided into two classes, contact cards and contactless cards. Contact cards need to be inserted into a card reader device to communicate. Contactless cards need only be in close proximity. They communicate through an antenna wound into the card. However, they also need battery on them. The fundamental component of a smart card is memory module. Smart cards can again be classified into two groups here, Memory-based cards and Microprocessor-based cards. As expected, memory cards are the smart cards with only memory on them. Typically about 1K-4K bytes of space for data. In some ways, they are not really smart. Microprocessor based cards on the other hand contain a processor. This increases security considerably, because data is never accessible to the external application, without going through the microprocessor. Microprocessor cards are the more widely used cards, having been deployed in access control, banking, wireless communication, etc. However, microprocessor cards also cost a little more than the simple memory cards. Some cards have an additional co-processor to expedite processing speed. We will re-visit this, a little later.

Operationally, smart cards behave as general purpose computers. They communicate with external devices using one of T0-T15 protocols. Essentially, these protocols let the card readers and the smart card have some form of flow control for their communication. The most commonly used ones are T0 and T1. T0 is designed for smaller data transfers where as T1 is designed for bulk data transfers. Both provide asynchronous half duplex communication.

Application : Smart cards are generally used for portable data storage and retrieval. However, the access to data has to be secure otherwise there is a

serious risk of data being handed to the wrong people. During the initial use of smart cards, they were primarily used for their portability. The need for security was not so much there. However, as the need to communicate across networks, grew, the need for security grew. Smart cards being the primary hardware tokens used, needed to provide security as well. Smart cards need to provide Access control, Authentication, Data integrity, and other security features, for the data on the smart card.

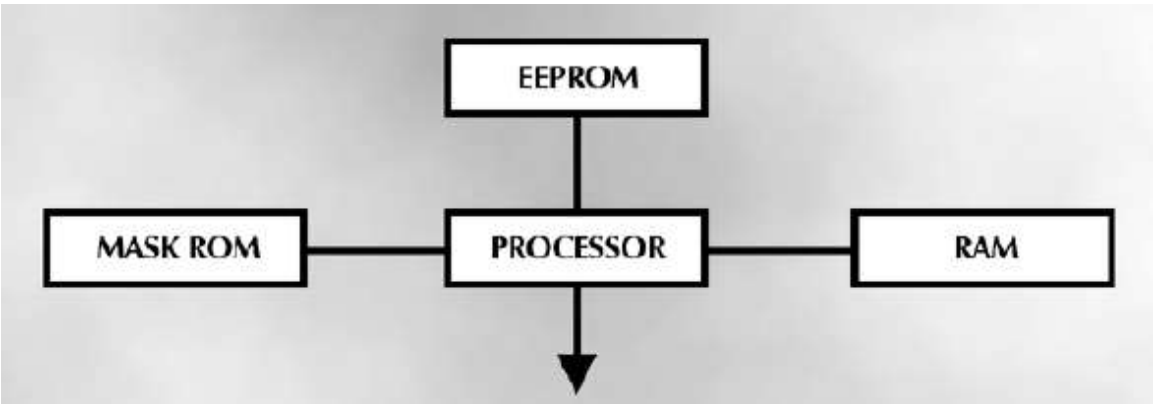

Figure 1: Smart card Architecture

As shown in the figure above, most smart cards contain a processor along with different types of memory. Mask ROM contains the operating system that is installed during the fabrication of the chip. This portion is read only and can not be changed once the chip comes out of production. The EEPROM is the non-volatile memory of the smart card and data can be written and read from various programs. This data is preserved even after the smart card is powered-off. Generally, a unique identification number is written into this part of memory, during the production. Later, a number of application programs are installed to assist in user level security. This data may include private keys, digital certificates, user names, and other data. The RAM part of the memory is more like the working space. It is used by the processor while executing programs. This RAM is similar to the one used in traditional PCs. The communication lines are the physical access mechanism for a card reader device to talk to the smart card.

Security : General requirements of any secure storage device are,

Access Control – Both logical and physical access.

Authentication – Only an authorized user can access data.

Integrity – Data on the smart card can not be tampered with.

Trusted Communication – Any external communication must preserve secrecy.

So, how is security implemented using a smart card? This is done by installing and running, a number of software programs on the smart card. When a user wishes to authenticate to a computer(a server or a desktop), they insert their smart card into the card reader attached to the computer. The software application on the

computer tries to read the data on the smart card by communicating in one of T0/T1 protocols. There are a number of steps involved here. Initially, the software talks to one of the managing(or master) modules on the smart cards. This redirects it to an appropriate application module. If the need is to read from the protected data, the application needs a Personal Identification Number(PIN) to unlock the data. Once the user enters this, then the application module can go ahead and read the protected data. Hence, it is upto the software program on the smart card to implement access control and authentication. Figure 2, shows this in pictorial form. In many practical applications, a user is limited to only a handful of wrong tries. In the Department of Defense's(DoD) Common Access Card(CAC) the number of wrong tries is limited to 3. Once 3 wrong entries are made, the software modules lock up the card.

One of the popular implementation of these software modules is the Java Card technology. Here, a Java Virtual Machine(JVM) is installed on the smart card, along with a set of applets for access by various applications. These applets inturn implement security features. One of the main features is the need to share data on the smart card. While doing so, smart cards encrypt the data before putting it on the communication line(Figure 1). To assist the smart card in implementing the security algorithm(like RSA, 3DES), usually, the main processor is accompanied by a co-processor. [7] discusses Java Card technology in great detail.

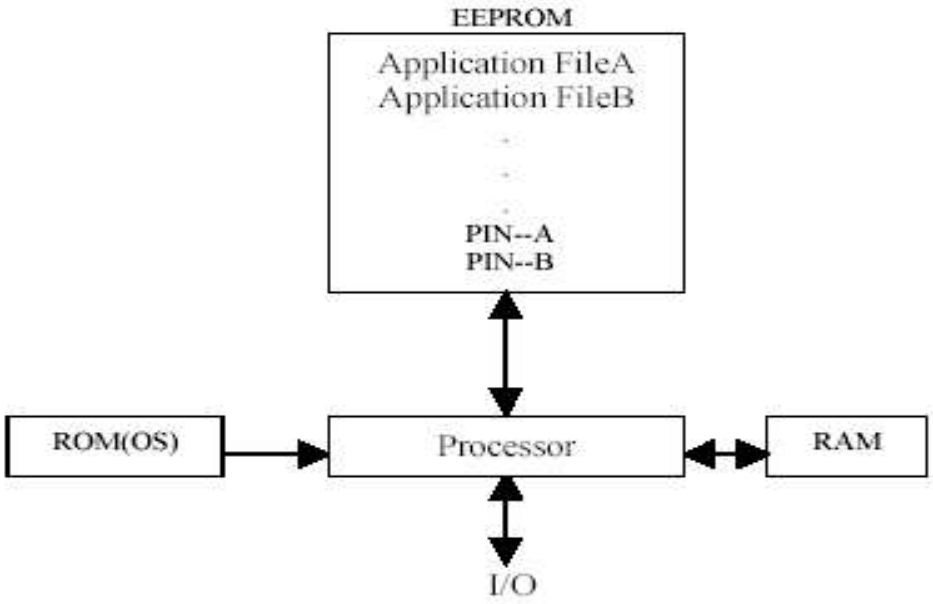

Figure 2: Smart Card Software Architecture

Security Vulnerabilities : Even with the secure architecture mentioned above several aspects of smart cards are vulnerable to attacks. In this section we will try to understand some of them.

Differential Power Analysis : In this method, the attacker tries to find out the power consumed by the smart card to get as much information as possible, regarding the calculations being performed. The approach is to insert a small

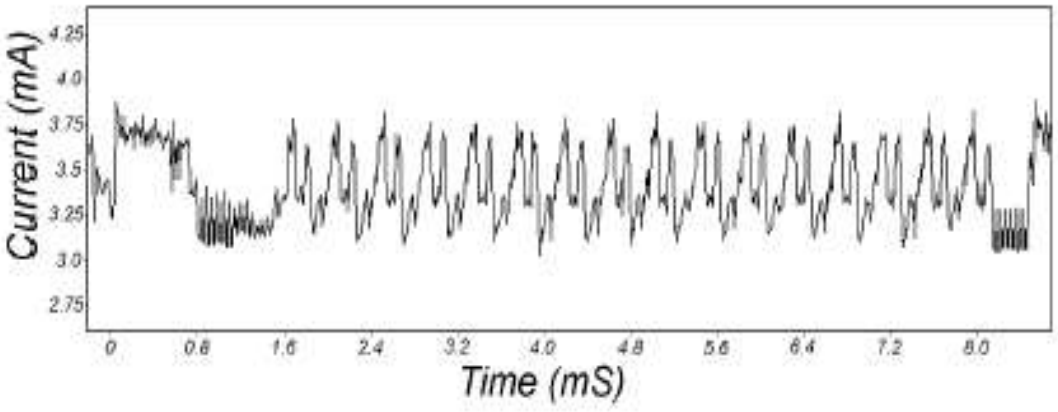

Figure 3: Current trace for a DES calculation[4].

resistor serially with the ground point. The current across the resistor can be calculated by measuring voltage and dividing it by the resistance(known value). A number of these current values can be collected by taking a lot of samples at high frequency intervals(of the order of Giga Hertz). Simple Power Analysis is a similar method which computes the power consumed, to predict cryptographic details. [4] discusses this in greater detail. Figure 3[4] above shows the current consumed during a DES operation.

There are a number of techniques to prevent such an attack. [4] proposes to avoid using routines which use secret keys for conditional branching. However, to implement this technique on cryptographic algorithms that involve key based branching, complex coding techniques may be needed, which can degrade the performance.

Attacks on Tamper Resistance :Smart cards have been popular for their tamper resistance. However, this is not extremely difficult to break. There have been a number of researches in exploring the tamper resistance of chip equipments in general and smart cards in particular. [1], [2], [3] explore these in greater detail. However, the basic idea behind all of these attacks is that they induce some sort of erroneous data using electromagnetic effects. Within tamper resistance attacks there are a certain class of attacks which require expensive semiconductor equipment to induce these errors. These are practically less feasible. However, there are another class of low cost attacks[2]. One of the technique used in these, is to apply a small glitch of high frequency clock. The idea is that smart card is made up of different Resistors, Capacitors and when a clock glitch is applied, only a set of them behave differently. This will make the processor behave differently and hence the processor calculations will be erroneous. [2] shows that this technique can be used to attack RSA, DES, RC5 and others.

Another kind of attack on tamper resistance involves inherent properties of the components of a smart card. For example, the EEPROM uses high voltages to erase the data after it is done with calculations. If the high voltage can be trapped,

then we know that the data being erased is residue of some calculation and hence we can back track it.

Other tamper resistance attacks involve varying the voltage during accesses to the security bit. If done correctly[3] it can clear only this bit without affecting other data.

There are a number of other invasive attacks on smart cards involving power and clock transients. A number of these attacks can be prevented by including a voltage or clock deviation detection circuitry. However, this will be at the cost of robustness since any environmental or other effects which vary these, will generate false alarms.

Software Attacks : Most smart cards are part of a much bigger security infrastructure. Consider the case of a user trying to authenticate to a server. The server will have stored the user's password in a table. During authentication, the smart card will send the same password after hashing it using a hash function and doing some simple mathematical operations(XOR). The server will remember the password as well as the hash function being used by a particular card. When the server receives this password, it hashes the stored value and compares it with the value it received from the smart card. If there is a match, it declares the user as authenticated.

With this technique, there are a number of possible vulnerabilities. An intruder with access to the servers and the network which the user is trying to authenticate to, can observe the traffic over a period of time and try to guess the password by storing a set of hash values. These kind of attacks are called insider attacks.

The other possible attack is that if an intruder finds out somehow(using one of the hardware techniques mentioned above) the password stored on the card, then he/she can observe a successful login attempt and try to guess the math operations and hence the hash function.

To reduce the risk of the software attacks such as the ones above, usually, smart cards store a password and a key to encrypt the password. However, access to the part of memory which stores the password and key, is again protected. In practice, smart cards require an additional PIN(Personal Identification Number) to gain access to the key. This increases the security by providing two factor authentication. That is, not only an intruder has to gain access to the smart card, but also the PIN.

Conclusion : Smart cards provide very portable and reliable data storage mechanism. However, they do have some security vulnerabilities. Some of these loopholes can be significantly reduced(like the software attacks), however, the differential attacks(or hardware attacks) can only be prevented by controlling the physical access to the smart card. That is, hardware attacks can be prevented if the smart cards are not allowed to be accessed by intruders and if a card is lost, the rest of the infrastructure is capable enough of disabling a smart card(remotely), once it is known that the smart card is lost/stolen. Bottom-line is that smart cards can be part of a security infrastructure, but they themselves can not provide end to end security.

References :

[1] Tamper-resistant Smart Cards Too Much To Ask For?
- Ville Taponen

[2] Low Cost Attacks on Tamper Resistant Devices (1997)
- Ross Anderson, Markus Kuhn

[3] Tamper Resistance – a Cautionary Note
- Ross Anderson, Markus Kuhn

[4] Differential Power Analysis
- Paul Kocher, Joshua Jaffe, and Benjamin Jun

[5] Security Pitfalls of an efficient remote user authentication scheme using smart cards.
- Manoj Kumar

[6] Smart Card Technology
- Dr. David B. Everett.

[7] Java Card Technology for Smart Cards, Architecture and Programmer's Guide - Zhiqun Chen