Enhancing Biometric Authentication with Data Protection

Anupam Dewan

Student ID: 3239797

e-mail: adew007@ec.auckland.ac.nz

Department of Computer Science

The University of Auckland

Abstract

This paper sets out to illustrate why using Biometrics with Smart Cards is a very secure security solution and why it is only now that these technologies are implemented together. The main focus of this paper will be on how the Biometrics Smart Cards might give some specific form of protection to some specific type of data (i.e. Biometric Data). Further we will be looking at an attack model, in which, what are the various attacks which are possible on the Biometric Smart Card are mentioned and finally a trusted authentication system is proposed which will make the present biometric authentication process more secure and safe.

1. Introduction:

Biometric Technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological and behavioral characteristics. Biometric technologies when used with a well designed ID system can provide the means to ensure that the user can trust the whole authentication process and can be sure that there will be no man-in-the-middle attack. Smart cards have the unique ability to store large amounts of biometric and other data, carry out their own card functions, and interact intelligently with the smart card reader. Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smart card and biometric technology.

The main focus of the paper is about the Biometric Smart Cards i.e. their security objectives, various possible attacks on them and will also be looking on how to make the Biometric Authentication process more safe and secure.

The rest of the paper is as follows: Section 2: Biometric Authentication Technology, Section 3: Biometric Smart Card, Section 4: Solution, Section 5: Conclusion.

2. Biometric Authentication

Biometric authentication works at a human to machine interface as one of the system is built of a secured and trusted system. To work it must verify the two things. Firstly it should verify that the biometric came from the person at the time of the verification and secondly, that it matches the trusted record of that person's biometric.

As stated by Dr. Jim Wayman biometric is "an automatic identification or identity verification of living, human individuals based on behavioral and physiological characteristics" [JPPR02].

Here the Behavioral Biometrics measures the habituated actions which are difficult to mimic, e.g. voice, gait and signature. Whereas, Physiological Biometrics measures the more static physical properties, e.g. fingerprints, patterns on iris and retina.

There are two processes involved in the biometric authentication. First is the enrollment process in which the system captures the biometric code of the person and then the person is enrolled. Second process is the verification process in which the system verifies the biometric data with the biometric code.

In this article I will not be discussing the Biometric Technologies, but the main focus of this paper will be to enhance the biometric authentication process along with the data protection.

2.1 Possible Attacks

The various attacks which can be possible on our whole Biometric Authentication Process are as follows: -

- Interception of communication between the Smart Card and the platform.
- Interception of communication between the platform and the Biometric Reader.
- Replacing the existing Biometric Reader with the malicious reader so that the reader can store the biometric data of the user and may send it to the attacker for further use i.e. may be for modification or fabrication.

- Attacking directly on the platform so that it is not able to verify the legitimate user. The reason for this is may be due to some personal motive. Indirectly the attacker is interrupting the user to gain access to the system.
- Attack on the Smart Card itself. Attacker can extract the biometric data from the card and then may try to modify or fabricate it.

To overcome the above threats we should see to it that the biometric code or the biometric data should not be transmitted in an unprotected manner between the smart card and the platform. A prescribed solution is presented in Section 4.

3. Biometric Smart Card

Implementing Biometrics on a Smart Card is a very new technology. The reason why more new developments are coming about now is due to the fact that the memory capacity in the modern Smart Cards has increased to make this a viable option. A Biometric Smart Card is the result of transferring a biometric image onto a smart card. The process typically includes the recording of a biometric template, verification of the biometric template, attaching a pin number and incorporating personal data.

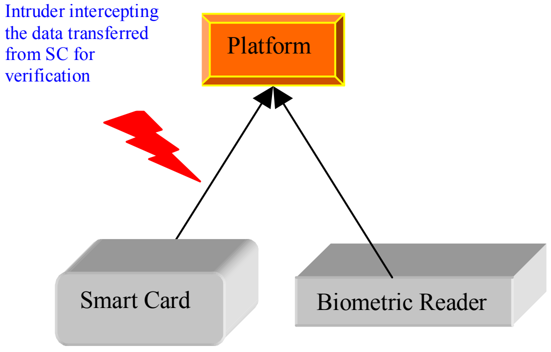
Biometrics can be used in a variety of ways on a Smart Card. They can be used to protect the information that is actually on the card. In this instance the Biometric would be used to verify that the person trying to access the data is really the person whose data is stored in the card. Another reason for storing the Biometrics on the card could be to identify the person to a computer, so they can verify that the Biometric on the card is that of the person trying to access the computer system. Biometrics could be stored on a Smart Card to be used as a passport, which would make it a lot more difficult for people to forge passports or to try and use someone else’s passport. So I think that Biometrics and Smart Cards can work together to bring an even better security solution.

One of the main advantages of using the Smart Cards with Biometrics is speed. This is because if we were implementing a Biometric solution without a Smart Card, then the person’s attribute has to be stored on a central database, which would take a lot of time to search, access and maintain. When using a Smart Card, the Biometrics data is stored on the card, so no time is wasted in searching a large database for the correct match.

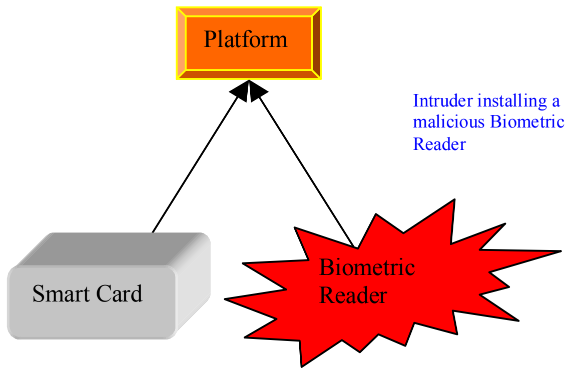
Under the coming sections we will be looking at how to make the Biometric data more secure inside the smart card, what are the various attacks possible on the smart cards and finally will look at how to prevent the attacks.

3.1 Security Objective

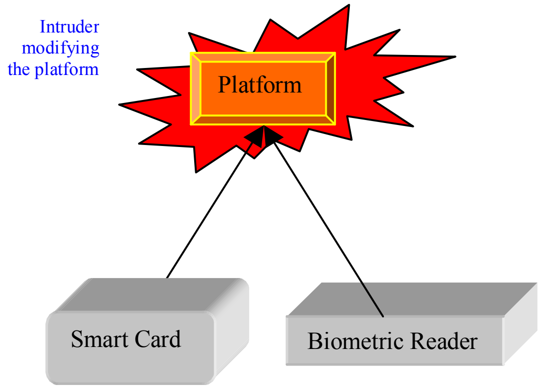
For centuries, security was synonymous with secrecy. In this world, still today the password and PIN is shared between the person and the machine. The machine can be anything like ATM or an EFTPOS. But secret passwords require a great deal of trust between parties sharing the secret. The people have no choice; they have to trust the system administrators or the persons who are looking after the security. But most of the computer break-ins which take place today are due to the compromise made by these people. Today the hacker or the intruder can easily attack the digital network and can extract the information. The intruder tries to find the vulnerability in the system and then tries to attack it.


Intruder intercepting the data transferred from SC for verification
Platform
Smart Card
Biometric Reader

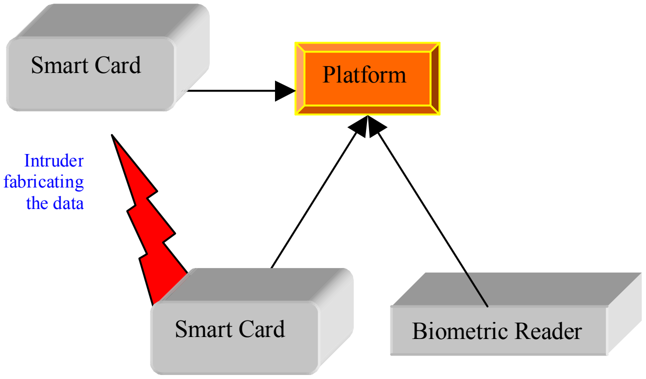
Interception



Interruption



Modification



Fabrication

If we talk in terms of the taxonomy given by Pfleeger then the threats which the intruder has on the security of the computing are Interruption, Interception, Modification and Fabrication (diagrams are presented on the previous page).

- Interception is because the intruder may try to intercept the communication between the Smart Card and the platform.
- Interruption is because the intruder may replace the current Biometric Reader with the malicious one, so that the reader can store the data and then the intruder can have the user's biometric data from there. In other words the intruder is interrupting the whole authentication process.
- Modification, here the intruder may modify the platform where the actual verification takes place; so that the user doesn't gain access to the system (may be this is the motive of the intruder). This also leads to Interruption. Both of these threats overlap each other so it is difficult to say that whether it is actually a modification or interruption.
- Fabrication, it is because the intruder may fabricate the user's biometric data and then gain access to the system with his biometric details, but under the name of the user. In this case the intruder will have anonymity.

To overcome the above mentioned attacks we will be considering an authentication model (discussed in Section: 4) which consists of three components: - Smart Card, Biometric Reader and a Trusted Platform (which performs the verification process).

Safety and Security both express the ability of a system to maintain its intended functionality under external influences. The term "safety" is used for resistance to random events, such as technical background or failure, and other effects resulting from environmental conditions. Security refers to resistance to intentional attacks such as espionage or sabotage. Obviously, a secure system is to a certain extent also a safe system, because if intentional actions are prevented, the same actions will also be prevented from happening accidentally.

The characteristics of data or data processing systems can be threatened by attackers (considering the Pfleegers Security Goals) are: -

Confidentiality – The attacker intends to obtain knowledge of confidential information.
Integrity - The attacker intends to modify data in such a way that the modification will not be noticed.
Availability – The attacker intends to make the data or the system unusable. Making the system unusable is also called a denial-of-service attack.

3.2 Smart Card Security

The Smart Cards seems to be a superior tool for enhancing system security and provides a place for secure storage. One of the security features provided by most of the smart card operating systems is the cryptographic facilities. They provide encryption and decryption of data for the card; some of them can even be used to generate cryptographic keys.

Besides cryptography, other software measures are also vital. The chip operating system and the chip application software must not contain any backdoors that would allow unauthorized access to secret data.

A smart card IC manufacturer's greatest problem is to ensure that secret information such as the cryptographic keys remains secret. Even the most severe software measures would be in vain if there were any possibilities that data could be read from the chip by direct access, bypassing the chip software. Because conventional IC's can be read, for example, with an electron microscope, special hardware security measures are built into smart card IC's. These hardware measures can be divided into passive and active measures.

Passive hardware security measures include shields, layered architecture, and scrambling. It is not too difficult for an attacker to disassemble the chip module and obtain access to the surface of the IC. Shields are additional metallic films covering the semiconductor surface. If an attacker wants to access the semiconductor, he needs to damage the shield, and this will cause the IC to cease working. The architecture of a Smart Card IC makes critical areas harder to access because they are placed in the deepest levels of the silicon. For example several other layers have to be penetrated before the ROM is reached.

Active hardware security measures allow the IC to detect attacks by using various sensors and to react, for example, by putting itself out of operation. The validity of supply voltage and clock frequency in particular are checked, because invalid values can cause malfunctions of the IC that can in turn enable an attacker to bypass other security mechanisms or to gather critical data directly. Another active measure is to check the integrity of the "passivation layer". This is a layer covering the entire semiconductor to protect it from oxidation. Its electrical resistance or capacity can be measured, which helps to detect any modification. As soon as the sensors detect the suspicious conditions, the IC can cease operation, switch to a special error state, or even delete all critical data. Although these sensors allow clever countermeasures, they work only as long as the chip is supplied with power. If someone tries to attack the chip without setting it into operation, it must be protected by the passive security measures.

3.3 Known Attacks on Smart Cards

The most obvious and direct attack on smart card is a physical attack on the card itself. In the case of a stored-value card, this sort of attack may even be carried out by the owner of a card. Physical attacks attempt to reverse engineer the card and determine the secret keys. Some of the attackers perform the logical non-invasive attacks while some of them attack the card physically.

In the paper by [RM96] the authors point out that "smart cards are broken routinely" and to the extent that their secure use requires tamper resistance, smart cards "should be treated with circumspection". The paper describes a number of smart card attacks, many of which can be carried out by amateur attackers with very limited resources. The attacks which are described in the paper include voltage manipulation, temperature manipulation, chip removal, UV light attacks and micro probing.

3.3.1 What is Physical Attack?

In order to perform the attack on the Smart Card one should need only a sharp knife and a little fuming nitric acid and acetone to expose the semiconductor surface of a smart card IC. In order to penetrate the passivation layer, micro probing needles can be employed. An attacker who understands the internal structure of a certain IC can disconnect the entire CPU except for the program counter and have it count all possible EEPROM addresses. Then he needs only to find the data bus in order to read all the EEPROM content [RM96]. This type of attack is known as a Physical Attack.

3.3.2 What is Logical Attack?

In the paper [RM96] several examples of attacking the smart card microcontroller by adjusting the voltage are provided. E.g. a widely known attack of PIC16C84 microcontroller is that the security of the controller can be clear with erasing the memory by raising the voltage VCC to VPP – 0.5V. An attack on DS5000 security processor is another example. A short voltage drop can release the security lock without erasing the secret data sometimes. Low voltage can facilitate other attacks as well; such as an analogue random generator used to generate cryptographic keys will produce an output of all 1's when the supply voltage is lowered slightly. This type of attack is known as Logical Attack.

Logical Attacks: All the important data of a smart card is stored in the electrically erasable programmable read only memory (EEPROM), and due to the fact that the EEPROM write operations can be affected by unusual voltages and temperatures, information can be trapped by raising or dropping the supplied voltage to the microcontroller [RM96].

3.3.3 SPA Attack

In *Simple Power Analysis* (SPA) an attacker directly observes device power consumption. It is known that the amount of power consumed by the device varies depending on the data operated and the instructions performed during different parts of an algorithms execution.

A trace refers to a set of power consumption measurements taken across a cryptographic operation. E.g. 1 millisecond operation sampled at 5 MHz yields a trace containing 5000 points [PJB99]. SPA can therefore be used to break cryptographic implementations details in which the execution path depends on the data being processed.

3.3.4 DPA Attack

Differential Power Analysis [PJB99] attack is more powerful attack than SPA attack because the attacker does not need to know as many details about how the algorithm is implemented. This technique also gains strength by using statistical analysis to help recover side-channel information. The objective of the DPA attack is to determine the secret key used by a smart card running the DES algorithm. This technique can be used to attack other cryptographic algorithms.

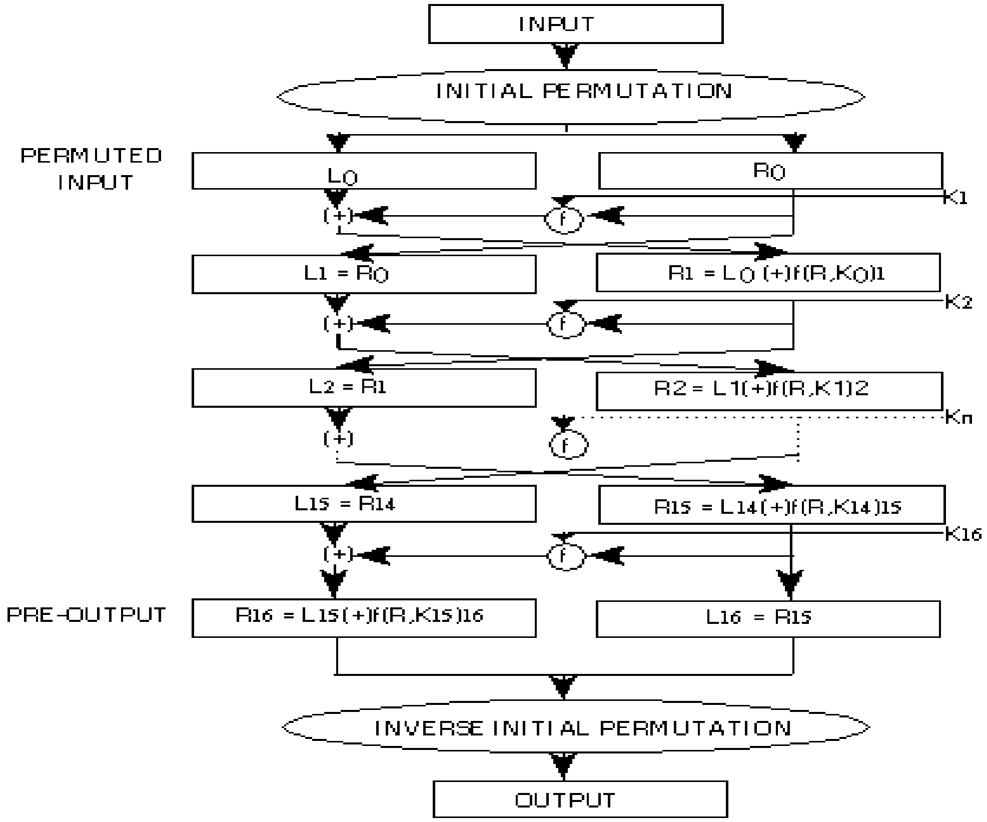
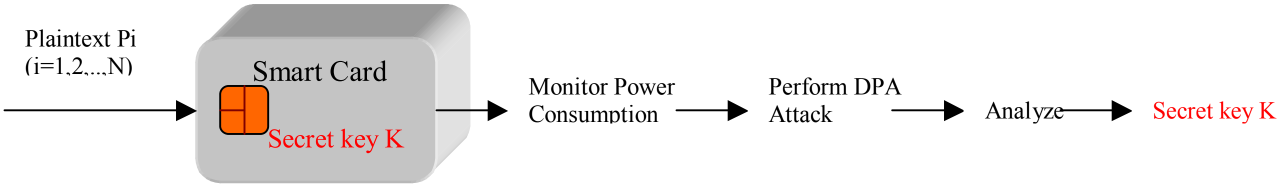


Fig 1: DES Algorithm [FI93]

In the Data Encryption Standard (DES) algorithm, it executes in 16 steps called "rounds". In each of these steps a transformation F is performed on 32 bits. This F function uses 8 non-linear transformations from 6 bits to 4 bits, each of which is coded by a table called "S-box". The DPA attack can be performed as follows (I am using a number 1000 as an example – as it has been taken by [PJB99]). To make it more understandable, I am mentioning the attack in steps.



DPA Attack

Step 1: We first measure the consumption in the first round, for 1000 DES computations. We give E_1, …, E_{1000} the input values of those 1000 computations. We give C_1,…, C_{1000} the 1000 electric consumption curves measured during the computations. We compute the mean curve – mc of those 1000 consumption curves.

Step 2: We focus on the first output bit of the first S-box during the first round. Let b be the value of that bit. The value of b depends on only 6 bits of the secret key. The attacker makes a hypothesis on the involved 6 bits. The attacker computes from those 6 bits and from the E_i – the expected values for b. This enables to separate the 1000 inputs E_1, ……, E_{1000} into two categories: those giving b=0 and those giving b=1.

Step 3: We now compute the mean mc' of the curves corresponding to inputs of the first category i.e. the one for which b = 0. If the mc and mc' show appreciable difference, we consider that the chosen values for the 6 key bits were correct. If mc and mc' do not show any sensible difference, we repeat step 2 with another choice for 6 bits.

Step 4: We repeat step 2 and 3 with a target bit b in the second S-box, then in the third S-box and so on till the eight S-box. As a result, we finally obtain 48 bits of the secret key.

Step 5: The remaining 8 bits can be found by exhaustive search or by analyzing one additional round.

Conclusion for DPA: -

- The attack needs to be performed on an operation where both of a part of the data and a part of the key come together i.e. Operation ($Data_{In}$, Key_i) = $Data_{Out}$

- Either Data_{In} or Data_{Out} of for that operation should be known. So, it means that the DPA attack in between the algorithm is not possible.
- An exhaustive 'search' on Key_{i} is needed. So the less bits Key_{i} has, the faster the attack will be.

4. Solution

The solution to the above mentioned problems is to make a "Trusted Biometric System". The main purpose of this system is to avoid the transmission, process and storage of the user's biometric code and biometric data on an un-trusted environment.

Here our system uses the TCP (Trusted Computing Platforms) [LSA02] and each TCP has at least one TPM (Trusted Platform Module). The main objective of this platform is to maintain users' privacy, provides the protection against the theft of the data, and moreover the uses can trust that his/her data is secure and his/her privacy will also not be breached.

As suggested by [LSA02] we can incorporate TCP in our existing system, in which the system uses the combination of Smart Cards, Biometric Reader and TCP. When the platform is booted it first checks the integrity of the Biometric Reader and if it fails to identify itself, the loading stops. Also the Smart Card can check the integrity of both the platform and the biometric reader (with the help of TPM).

Now in brief how this system works: - The platform (TCP) has a mutual authentication with the smart card and the biometric reader. The smart card can check the integrity of the platform and the biometric reader. If the smart card is satisfied with the integrity of both, then the platform (TCP) authenticates the smart card's identity and then obtains the biometric code from the smart card, and also the user gives his biometric data to the biometric reader which then transfers it to the TPM in a secure manner. Then finally the TPM matches the biometric code with the biometric data, and if it matches the user is granted the access.

The main advantage of using the system is that all the data is transferred in a secure manner, and the data is transmitted in the encrypted form. To learn more about the encryption techniques see [LSA02].

Now whereas the SPA and DPA attacks on Smart Cards are concerned, the possible solution for that is to use microcontrollers with low power consumption and additional noise generators for power “blurring”. The useful information is hidden in between the irrelevant but strong noise which has to be extracted by advance signal analysis method.

5. Conclusion

This document illustrated that a Smart Card is:

- A plastic card similar in size to a credit card that has a computer chip and a printed circuit embedded within it.

It also explains that Biometric is:

- A physical attribute or behavioral characteristic of a person which can be used for authentication or verification.

These technologies can be used either separately or together to provide a reliable security solution. When they are used together they are even more secure, as they can provide a multiple layer security solution. The other advantage of using them together is speed and the fact that the solution can be a small implementation or a worldwide solution.

Although there is a large initial outlay to have these solutions installed, the benefits that you gain from them can be immeasurable. In business today, if a security breach occurs, then customers can lose faith and move to another organization for their products or services, but if you have a good security solution installed such as Biometric Smart Cards and use of Trusted Platforms, then the clients can be satisfied that their information is safe and moreover they can also trust the organization.

References:

[JPPR02] John Armington, Purdy Ho, Paul Koznek and Richard Martinez, Biometric Authentication in Infrastructure Security, Infrasec-2002, Proceedings: LNCS 2437, pp. 1-18, Springer 2002
Available:http://link.springer.de/link/service/series/0558/papers/2437/243700001.pdf

[RM96] Ross Anderson, Markus Kuhn, Tamper Resistance – a Cautionary Note, proceedings of the Second Usenix Workshop on Electronic Commerce, pp. 1--11, November 1996
Available:http://www.cl.cam.ac.uk/users/mgk25/tamper.pdf

[LSA02] Liqun Chen, Siani Pearson, Athanasios Vanvakas, A Trusted Biometric System, HP Laboratories, Bristol, HPL-2002-185 July 15th, 2002
Available:http://www.hpl.hp.com/research/tsl/external%20publications/tech%20reports/HPL-2002-185.pdf

[PJB99] P.Kocher, J.Jaffe, and B.Jun, Differential Power Analysis, Crypto99
Available:http://www.cryptography.com/resources/whitepapers/DPA.pdf

[FI93] Federal Information, Data Encryption Standard (DES), Processing Standards Publication 46-2, 1993 December 30
Available:http://www.itl.nist.gov/fipspubs/fip46-2.htm