TDDC03 Projects, Spring 2007

“Security and privacy issues for E-Passports”

Fahad Adeel <fahad066@student.liu.se>
Waqar Bajwa <wagba713@student.liu.se>

Supervisor: Viiveke Fåk

Abstract

As time is passing, things are getting better and technologies are evolving to meet the need of the time. Electronic passports are one of that and for E-Passports the security and privacy issue is the very first problem we face. We will give a brief introduction and will discuss are the technologies (RFID) and (Biometrics) which used in E-Passports. We will analyze the Biometric E-Passport system. The idea behind the report is to look at the security aspects and try to solve them. We will end the report with the modifications and enhancements that have been made in recent years and come up with our conclusion.

1. Introduction.

An E-Passport or a Biometric Passport is a combined paper and electronic identity document that uses biometrics to authenticate the citizenship of a person. The passport's confidential information is stored on a tiny RFID (Radio Frequency IDentification) chip which is an automatic identification method. A basic RFID device, often known as "RFID tag" consists of a tiny, inexpensive chip that transmits a uniquely identifying number over a short distance to a reading device, and thereby permits rapid, automated tracking of objects. The RFID chip contains the biometric and personal information. The ICAO (International Civil Aviation Organization) of the United Nations defines the biometric standards to be used in passports, it provides a guideline for E-Passports on what features could or should be implemented. The current staged biometrics which is used for this type of identification system is facial recognition, fingerprint recognition, and iris scans.

Figure 1.1: Biometric feature of thumb

Figure 1.2: RFID tags

Together RFID and biometric technologies promise to reduce fraud, ease identity checks and enhance security. At the same time, these technologies raise new risks which contain different problems, like data confidentiality and integrity in E-Passports [9], which are:

- Biometric feature leakage.
- Clandestine Scanning and Eavesdropping.
- Cryptographic weaknesses.

Leakage of "Biometric" features (e.g., fingerprints) can be jeopardous, since, it allows an imposter to use the fake identity and it permits the acceptance of invalid users. "Eavesdropping" of data also breaks the rules of security. For instance, eavesdropping enables a pretender to copy a passport complete with chip data, or reveal data, which can then be used to make duplicate passports.

Cryptography in E-Passports protects eavesdropped or skimmed data from being understood by an imposter. Since, the stolen data are in static form, there is a risk of skimming and cloning. This risk exists also for encrypted data and if a faker gets hold of the key, then he can use that key to make a fake passport.

Both RFID and biometrics are highly privacy sensitive technologies that carry sensitive data on E-Passports. Therefore protecting E-Passport data against unauthorized access and giving privacy and psychological comfort to the user is a crucial part of the security of the entire system.

We have analyzed and discuss the above mentioned problems, which we identified in our minds and through our studies. Our main focus is to study the insecurity problems in E-Passports and propose new ideas or enhancements to defeat them. We have identified security and privacy threats in E-Passports which are running globally, and then we evaluate emerging and impending E-Passport types with respect to these threats.

If we succeed to minimize or to overcome these threats and vulnerabilities, then it can create a large impact on the deployment of E-Passports worldwide.

The special features of an Electronic Passport are:

- Securely stored biographical information and digital image that are identical to the information that is visually displayed in the passport.
- Contact less chip technology that allows the information stored in an E-Passport to be read by special chip readers at a close distance.
- Uses digital signature technology to verify the authenticity of the data stored on the chip. [7]

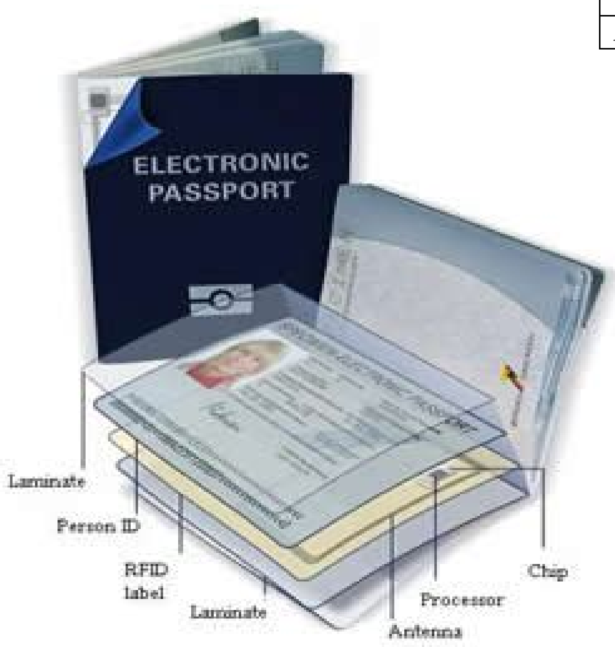

Figure 1.3: E-Passport

2. Evolution of E-Passports.

The first country in the world to issue E-Passports was Malaysia in 1998 and it was followed by many countries. These countries, along with the other early adopters, now use the ICAO standard passports.

After the 9/11 disaster and due to losses and cases of stolen passports in U.S and in other countries, there is a rapid increased demand for biometric passports deployment in different countries. Then all the International community through the support of International Civil Aviation Organization (ICAO) adopted E-Passports which contain smart chips on which data can be stored and read wirelessly by chip readers. The U.S made obligatory that 27 Nations of VWP (Visa Waiver Program) must issue E-Passports till Oct, 2006 so that their citizens can continue to enter the US without first obtaining a visa.

Country	Biometric	Deploy
Malaysia	Finger Print	1998
Pakistan	Finger Print	2003
Belgium	Digitized Photo	2004
Netherlands	Digitized Photo	2005
Sweden	Digitized Photo	2005
Germany	Digitized Photo	2005
USA	Digitized Photo	2005
Australia	Digitized Photo	2005

Table 1:
Major deployment of e-passports in different countries

3. Risk and Security issues.

RFID tag reading is not a visible process. It provides us end-to-end communication encryption and database security. As we have mentioned earlier, there are different types of security issues and threats in E-Passports. Here is the summary of the major points we touch on:

3.1 Biometric feature leakage:

Biometric technology in E-Passports identifies individuals automatically by using their biological or behavioral characteristics. An adversary can steal biometric features of a person very easily, if thumbprints are used. He can use fake prints and can deceive biometric thumb scanners.

Leakage of biometric data on E-Passports poses its own special risks: compromise of security both for the E-Passport deployment itself, and potentially for external biometric systems as well. And hence some of biometric features are not acceptable 100% till yet, it gives us the result of FAR and FRR.

Biometrics are not secrets, they are properties of your body that you slough off all day long, when you are eating lunch, or driving your car, or opening the door. As a result, each of us leaves a trail of biometric signatures everywhere we go, creating many chances for theft of biometric information. [1]

The biometric data leakage becomes an issue when automation is to be introduced into passport controls.
When a machine is supposed to take part of the control, the persons completing the authentication would not be so concentrated. [2]

3.2 Clandestine Scanning and Eavesdropping:

E-Passports are vulnerable and open to attack by an eavesdropper, which means clandestine reading of their contents. It is well known that RFID tags can be remotely read via commercially available sensors and antennas with some basic receiving equipment. RFID readers can broadcast RFID tag data over long distances – often up to hundreds of meters away. It is difficult to shield the radio emissions of readers effectively without impeding their use. This is a bigger threat to E-Passports because an adversary can gain accessory knowledge and can steal sensitive information including date of birth, place of birth etc, and it is hard to detect.

3.3 Cryptographic Weaknesses:

The data stored on RFID chips is encrypted in order to avoid misuse of data. The reader (Immigration Officer) makes optical contact with the passport and scans the name, date of birth, passport no and necessary information to derive a cryptographic key with the following functions:

1) It allows the passport to establish that it is talking to a legitimate reader before releasing RFID tag information.
2) It is used to encrypt all data transmitted between a user and passport. [10]

Major weaknesses are a weak key, which used with a cipher (encrypted data) makes the cipher behave in an undesirable manner which results in disclosure of encrypted data so that RFID tag information is released. Similarly Password Authenticated Key Exchange is a method when two or more parties interact with each other using known passwords and transfers the cryptographic key information. The weakness due to this method is it unauthorized parties (not parts of the communication) intrude in between by guessing passwords. Cryptographic keys are only used to avoid man in the middle attacks, eavesdropping and tampering with data.

Encryption can make it impossible to understand for an eavesdropper what the leak of data is but there is a risk of skimming and cloning of encrypted data that can be copied to a fake passport.

The cryptographic weakness is about no key revocation. Once the key is obtained by a reader it can be stored and reused anytime later. There is no possibility to change the key although the passport validity is supposed to be 5 to 10 years. This long time presents another danger- cryptanalysis advance during the time. [3]

3.3.1 Skimming and Cloning:

Without protective measures, skimming is where the data in the RFID chip is copied to a duplicate document without the owner's knowledge. Cloning of E-Passports is a major security issue, as people with similar faces could possibly use the same passport.

4. Modifications and Enhancement.

Privacy activists in many countries question and protest the lack of information about exactly what the passports chip will contain, and whether they impact civil liberties.

The main problem which is most often pointed out is that data on the passports can be transferred with wireless RFID technology which can become a major vulnerability. Although this would allow ID-check computers to obtain your information without a physical connection, it may also allow anyone with the necessary equipment to perform the same task. If the personal information and passport numbers on the chip are not encrypted, the information might wind up in the wrong hands. [4]

One of the simplest measures for preventing unauthorized reading of E-Passports is to add RF blocking material to the cover of an E-Passport. Materials such as aluminum fiber are opaque to RF signals and could be used to create a Faraday Cage, which prevents reading the RFID device inside the E-Passport. Before such a passport could be read, therefore, it would have to be physically opened.

To prevent skimming and eavesdropping of data, Basic Access Control (BAC) is employed. BAC is similar to a PIN used in ATM or credit card transactions. In the case of the electronic passport, characters from the printed machine-readable zone of the passport must be read first in order to unlock the chip for reading. Thus, when an E-Passport is presented to an inspector, the inspector must scan the printed lines of data in order to be able to read the data on the chip. [6]

The new passports use Public Key Infrastructure (PKI) technology that prevents the chip from being altered; thus, providing a higher level of security for the passport. Access to the data on the chip requires the use of an official public key to ensure that the data has not been altered and that it was written to the chip by the Department of State. Although some experts have advised that surreptitious reading of data from the chip cannot be achieved beyond prescribed distances, the department intends to issue all electronic passports with an anti-skimming feature built into the passport. "In anti-skimming feature application, the chip is designed to operate within 10 centimeters (less than 4 inches) of a chip reader using appropriate public keys". The device would prevent any reading of data on the chip while the passport is not being used. [8]

5. Conclusion.

As we have discussed in our security issues, there are still many loop holes in E-Passport. Biometric images of an entity can be copied from many sources and reused to deceive thumb print scanners installed at airports. Similarly in Cryptographic weaknesses, a password guess and detection during exchange of encryption key results in misuse of encryption keys.

These all flaws are very serious and harmful, although recent passports are providing much security but still not bringing out 100% result, and in this sensitive matter, one cannot afford to disclose valuables. Hence, protection of your identity is something that is saving the asset of your life.

We can overcome these flaws if we recommend Iris Scans which should be mandatory in replacement to Finger scans and Facial recognition.
In password guessing the communication could be more secure if a special codes exchange between genuine users, which identifies that the user at other end is genuine.
To combat the skimming of your E-Passport, you should be very careful while opening your E-Passport in front of others and limit your E-Passport use to be just between you and the required authorities. E-Passports may provide valuable experience in how to build more secure and more private identification platforms in the years to come.

6. Acknowledgement.

We would like to say thanks to our teachers who motivate us and for their helpful discussions, our class fellows who encourage us and to our university staff who allow us to do this task and help us out in every matter.

7. References.

[1]http://www.pcworld.com/article/id,103535-page,1/article.html
[2]http://www.buslab.org/index.php/content/view/24733/62
[3]http://www.buslab.org/index.php/content/view/24733/62/
[4] http://en.wikipedia.org/wiki/Biometric_passport
[5] http://en.wikipedia.org/wiki/Biometric_passport
[6]http://travel.state.gov/passport/eppt/eppt_2788.html#Twelve
[7]http://travel.state.gov/passport/eppt/eppt_2788.html#Three
[8]http://travel.state.gov/passport/eppt/eppt_2788.html#Three
[9] http://eprint.iacr.org/2005/095.pdf
[10] http://eprint.iacr.org/2005/095.pdf