Final Report

Biometric Passport: Security And Privacy Aspects Of Machine Readable Travel Documents

Swiss Joint Master of Science in Computer Science

Students Name: Hesam Kolahan, Tejendra Thapaliya
Students Number: 08502437, 09506320
Course Name: Electronic Government
Department: Department of Informatics
Course Code: 53534
Supervisor: Prof. Andreas Meier, Luis Teran
Date: 1 December 2011
Abstract

E-passports are widely deployed in most of the developed countries that stores the biometric information on a tiny Radio Frequency Identification (RFID) chip. The stored information is used to authenticate the identity of individual via wireless interface to reader. E-passport uses two technologies, RFID and Biometrics. The objective of the e-passport is to provide strong authentication, prevent identity fraud issues and border control. Even though, Biometrics is advanced authentication mechanism, it leads to many privacy and security issues. Major privacy and security issues on RFID chips were identified and analyzed. Similarly, Biometric security threats that applied to e-passport have been analyzed and some recommendations were provided. Cryptography technology and several protocols are used to countermeasure the threats and attacks. Due to increase in standard of attack level and insufficient specification for e-passports are creating difficulties in providing security goals.
# Table of Contents

1. **Introduction** .......................................................................................................................... 4
   1.1. Objective and Problem Definition .................................................................................. 4
2. **Biometrics** ............................................................................................................................ 4
   2.1. Machine Readable Travel Document (MRTD) ......................................................... 4
   2.2. E-Passport .................................................................................................................. 6
   2.3. Radio Frequency Identification (RFID) ....................................................................... 8
   2.4. Chip Inside Symbol ................................................................................................. 9
3. **Privacy and Security Issues** ................................................................................................. 10
   3.1. Eavesdropping ......................................................................................................... 10
   3.2. Reverse Engineering ............................................................................................... 10
   3.3. Clandestine Scanning and Tracking .......................................................................... 10
   3.4. Cloning ..................................................................................................................... 11
   3.5. Biometric Data-Leakage ........................................................................................... 11
   3.6. Cryptographic Weaknesses ....................................................................................... 11
   3.7. Skimming .................................................................................................................. 11
4. **Biometric System Model** ..................................................................................................... 12
5. **Biometric Security Threats** ................................................................................................. 13
6. **Cryptography in e-passports** ............................................................................................... 14
   6.1. The ICAO specification ............................................................................................. 14
   6.2. Passive Authentication (PA) .................................................................................... 14
   6.3. Active Authentication (AA) ..................................................................................... 15
   6.4. Basic Access Control (BAC) ..................................................................................... 15
   6.5. Extended Access Control (EAC) ............................................................................... 15
   6.6. Cryptography Threats ............................................................................................... 16
7. **Discussions on Security and privacy risks with the E-Passport** ........................................... 16
8. **Recommendation** .................................................................................................................. 17
9. **Conclusion** .......................................................................................................................... 18
10. **References** .......................................................................................................................... 19
List of Figures

Figure 1, Mandatory and Optional Data Elements defined for LDS............................................................. 6
Figure 2, Biometric Passport......................................................................................................................... 7
Figure 3, RFID System ................................................................................................................................. 8
Figure 4, RFID Circuit................................................................................................................................. 9
Figure 5, RFID Symbol ............................................................................................................................... 9
Figure 6, Biometric System Model............................................................................................................. 13
1. Introduction

Biometric technology is becoming the base for secure authentication of personal identity. Many countries started to issue E-passports with an embedded chip containing biometric data. International Civil Aviation Organization (ICAO) started to work on MRTD since 1968. The concept of Machine Readable Zone (MRZ) was introduced in 1980 which contains two machine readable lines at the bottom of the identity page of passport. Finally, ICAO started to operate on biometrics in 1997 [1]. As the level of security and transaction fraud increased the need for more secure authentication technologies have to be deployed. The latest biometric standardized contains biometric features such as fingerprint, facial and iris recognition and enhances the security mechanisms.

Even though, biometric (RFID based passports) is very advanced authentication mechanism, it can lead to several privacy and threat issues. RFID is a technology and device that uses radio waves to transfer identifying data from an electronic tag. Since, the data stored in RFID chip is transmitted in wireless way, it is vulnerable to be attacked at a distance.

The attack on September 11, 2001 in United States of America warned government worldwide to handle and review the security and border control issues that was in practice. Use of biometrics globally was one of the reliable technologies to keep the identification of citizens. ICAO began to research on biometric passports in 1997, and has developed a set of international recommendations for the development and specification of globally interoperable biometric standards. With the advancement in biometric technology, ICAO introduced a new concept to embed and RFID chip on passports 2004 [2][3][4]. Since, then e-passport system has become a global issue and much work has been carried out to make it more secure.

1.1. Objective and Problem Definition

E-passport contains highly sensitive data of an individual. Protecting biometric and biographical data is very important to the value and consistency of an authentication system. Therefore, these data should be protected against unauthorized access and the quality of data protection mechanism should be taken into account. Security mechanisms that are implemented in RFID chips and biometrics data are vulnerable. The E-passports came into operation since 1998 but still the technology is not free from attacks.

2. Biometrics

2.1. Machine Readable Travel Document (MRTD)

The International Civil Aviation Organization (ICAO) started to work on MRTDs in 1968. The first standard specifies a discrete MRZ to be optically scanned in 1980. The essential information such as the document number, validation date, name, sex, date of birth, and citizenship of an
individual are stored in it. ICAO started to expand its works on adding more data, including biometrics, since 1997.

The basic requirements that MRTD must include a facial image, a digital copy of the MRZ and digital signature of the issuing country. The digital signature comes with a Public-Key Infrastructure (PKI). The ICAO standard provides a Passive Authentication (PA) protocol for data authentication, optional Basic Access Control (BAC) for protection of chip from unauthorized access and an Active Authentication (AA) for the validation of the chip.

2.1.1. Logical Data Structure for MRTD

A standardized Logical Data Structure (LDS) is needed for global interoperability and the ICAO’s e-passport guideline provides details on how data should be stored in a microchip. Data Group (DG) is used for grouping the logical data together and collectively stored in a LDS. The ICAO guideline divides data elements into 19 data groups and the LDS is classified into three parts [5]. The figure 1 shows the mandatory and optional data elements defined for LDS.

- **Mandatory**

This part contains the data defined by the issuing state or organization. It includes the details recorded in the MRZ such as passport number, passport bearer’s name, nationality, date of birth, date of expiry, encoded facial biometric image and checksum of individual data elements which are used for deriving the session key.

- **Optional**

This part contains the data defined by the issuing state or organization. It includes encoded identification features (face, finger and eye), displayed identification features (digital signature) and encoded security features (contact details, proof of citizenship and endorsements).

- **Optional**

This part contains data defined by the receiving state or approved receiving organization data such as details for automated border clearance, electronic visas and other travel records.
2.2. E-Passport

In 1988, idea of e-passport was introduced by Davida and Desmedt [6][7]. A Biometric passport, in simple known as an e-passport, is a paper and electronic identity credential which contains
biometrics features to authenticate the citizenship of travelers. It contains a chip and antenna enclosed in front or back cover, or central page. The chip is used for storing the user’s information printed on the personal details page of passport and biometric characteristics from the provided photograph. An e-passport also contains some biometric identifiers depending on various countries choice and technical evolution. The information stored inside the chip follows the recommended file formats and communication protocols established by the ICAO doc 9303[2][3][5]. The ICAO considers currently standard biometrics for identifications are facial recognition, iris scan and fingerprint. The ICAO e-passport guideline explains the integration of biometric chip with MRTDs as well as uses standards like ISO 14443, ISO11770, ISO/IEC 7816, ISO 9796, RSA, ECDSA and DSA.

Figure 2: Biometric Passport
2.2.1 Working Mechanism of Biometric Passport

An e-passport is basic document to identify and improve the security issues at border control. The border security officer uses MRZ reader to scan the MRZ part of e-passport to retrieve the embedded information. Then, the stored information is obtained from the contact less chip by putting the e-passport near to e-passport reader. Finally, verification of data is performed using PA, BAC mechanism for data encryption and integrity verification using either passive or active authentication. PA is compulsory where as BAC and AA are optional.

2.2.2 Special Properties of E-passport

- Biographical information and biometric information are securely stored which are identical to the information in the passport.

- Contactless chip technology that lets the stored information to be retrieved by chip readers at a close distance.

- Digital signature technology for verification of authenticity of the data stored on the chip.

2.3 Radio Frequency Identification (RFID)

RFID is sometimes called dedicated short range communication (DSRC). RFID is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency (RF) area of the electromagnetic spectrum to identify uniquely and track objects. RFID chips are being used everywhere such as tracking animals, inventory tracking devices, to start cars, especially in e-passports [8].

Figure 3: RFID System
RFID system contains three components: an antenna, transceiver and a transponder. The transponder is activated when it receives the signal from the antenna and after activation, transmits data back to the antenna. RFID systems are one of the most ubiquitous computing technologies to enhance the quality of service and to prevent theft in many applications. RFID tags which do not have onboard batteries are known as passive RFID tags. They use power from reader in order to be activated and start to broadcast the signals continuously within the certain range from few centimeters to few feet. On the other hand, active RFID tags with internal battery can transmit the signal hundreds of feet.

Figure 4: RFID Circuit

2.4. Chip Inside Symbol

Based on ICAO definitions, a Machine Readable Official Travel Document has a contactless IC imbedded in it that can be used for biometric identification of the MRtd holder. Therefore, all eMRtds shall carry the following symbol. The symbol shall only appear on an MRTD that contains a contactless integrated circuit. The recommended dimensions of the symbol are shown as below [5].

Figure 3: RFID Symbol
3. Privacy and Security Issues

Security in e-passport system has become a crucial importance due to the deployment of RFID system. Contactless and RFID chips use the wireless technology which is vulnerable to be exposed at a distance. The attacks can take place at communication network, chip or at backend system. E-passport guarantees confidentiality, consistency and authenticity of information based on some cryptographic tools. Even though, biometric system provides effective and better aspect for user authentication compared to others but it is not fully protected. In recent years, some weaknesses are evolving related to data privacy issues. Several attacks at hardware and software levels are possible. The most common attacks are as follows: Eavesdropping, Reverse Engineering, Clandestine Scanning and Tracking, Cloning, Biometric Data-Leakage, Cryptographic Weaknesses and Skimming.

3.1. Eavesdropping

It is the process where attacker secretly listens to the communication link and intercepts the information by using unauthorized device during the communication between chip and legitimate reader. This is a kind of passive attack and very hard to acknowledge because there is no emission of powered signals. It has been reported that up to at least of 2 meters attacker can eavesdrop on the communication network of RFID cards. The deployment of E-passport is not limited only for airports but in various commercial applications which facilitates the attacker a wide scenarios for eavesdropping.

3.2. Reverse Engineering

It is the process of taking the technological principles of a device, object or system apart to figure out how it works. Biometric chip uses a unique id as a private key that is hardcoded in chip manufacturing process so are very difficult to reverse engineer. However, the attacker can reverse engineer if he/she has the sound technical knowledge and has access to equipment which is not commonly found in commercial market. Potential reverse engineering of biometric template that could lead to reconstruction of the images of physical characteristics is an important issue. Although it has been considered to be impossible, research is going on to reduce the set of potentially matching images of the physical characteristic using the template.

3.3. Clandestine Scanning and Tracking

Clandestine scanning is defined as the secret way of reading the electronic data of an identity card without the permission of the card holder. Private information like as name, date and place of birth, and nationality can be retrieved easily by anyone having the reader. Clandestine tracking is an ability to locate an individual and it can easily reveal the location privacy. Clandestine tracking is more harmful compared to clandestine scanning because the attacker can keep track
of information in a global scale and without physical presence. To minimize clandestine scanning, a Faraday cage has been suggested to protect the e-passports [9].

3.4. Cloning

Card cloning is the way of acquiring the data from an authorized identity card and making an unauthorized copy of the captured sample in a new chip. In Johns Hopkins University and RSA Labs, the researchers published cloning result of a cryptographically-protected Texas Instruments Digital Signature Transponder (DST) which was used to buy gasoline and activate a car's ignition [10]. Active authentication is used as the counter measure for cloning threat but it can be bypassed by amending the EF.COM file of the passport chip.

3.5. Biometric Data-Leakage

Most of the biometric data are constant. Once, if the biometric data are compromised, replacement is not possible. Because of this property, it is widely used in e-passports to enhance privacy and security concerns. One of the technic to increase data security is to use data-hiding. In order to protect biometric data from modification and attacks, watermarking-based multimodal biometric approaches are widely used. Watermarking-based multimodal biometric system with two levels of security is presented by Vatsa et al. individual verification and biometric template protection [2]. In the proposed algorithm, the iris template is watermarked in the face image which makes the face image visible for verification and the watermarked iris for cross-authentication and biometric data security.

3.6. Cryptographic Weaknesses

Cryptographic technologies have been deployed in biometric smart cards in order to store and transfer the information in secure manner. Biometrics are widely used for automatic recognition of an individual depending on the behavioral or physical characteristics. Barni et al. [11] proposed a new scheme for preserving authentication based on fingerprints that uses ElGamal cryptosystem for biometric comparison in encrypted domain. The scheme has no facility for key sharing and only used for authentication. The authentication protocol for e-passport by Abid and Afifi [12] based on elliptic curve cryptography is more theoretical without experimental evaluation. Finally, it is concluded that there are some weakness on cryptography relied by ICAO.

3.7. Skimming

A skimming is the act of obtaining encoded data without the consent of users by using electronic storage device. The data from e-passport can be retrieved by beaming power at the passport within a few inches or at most a few feet. However, if the reader broadcasts the signal with high power the range can be extended.
4. Biometric System Model

By showing a generic biometric system model and its different modules, the ways of attacks to the system must be understandable [13].

- **Sensor**

The sensor (scanner) module is used to acquire the biometric data such as fingerprint and iris recognition of an individual in appropriate formats.

- **Feature Extractor**

The feature extractor module operates on the signal sent from the scanner module. It extracts a feature set that presents the given data.

- **Stored Templates**

The stored templates module is a database to store pre-acquired features sets (templates) during users’ enrolment.

- **Matcher**

The matcher module receives feature sets from the feature extractor module and compares them with the templates stored in the database that provided by stored templates module. Match scores are generated after each comparison and then it processes the scores in order to verify the identity of an individual. Making the decision is operated by this module in order to response “Yes” if there is a match or “No” if there is no match. Therefore, this module is the main module in a biometric system.

- **Application Device**

The application device module acts based on matcher answer. If it receives a “No” then access denied happens and if it receives a “Yes” then granted access occurs.
5. Biometric Security Threats

- **Fake Biometric**

In this attack, the attacker physically destroys the recognition scanner and causes a Denial of Service (DoS). The attacker can also create a fake biometric trait to bypass facial or fingerprint recognition systems by using an artificial finger or inject an image for sensing element. The problem with most of the fingerprint scanners used these days is distinguishing between a real finger and a well created dummy finger [14].

- **Replay Old Data**

In this attack, the attacker sniffs the communication channel between the scanner and the feature extractor to steal biometric traits. Then, the attacker can replay the stolen biometric traits to the feature extractor to bypass the scanner.

- **Override Feature Extractor**

In this attack, the attacker can replace the feature extractor module with a Trojan horse to operate malicious activities [15].
• Synthesized Feature Vector

This attack is similar to the attack Replay Old Data. The attacker sniffs the communication channel between the feature extractor and the matcher to steal feature values of an authorized user and replay them to the matcher.

• Override Matcher:

This attack is similar to the attack Override Feature Extractor. The attacker can send commands to the Trojan horse to provide high matching scores (to send a “Yes” to the application) to bypass the biometric authentication system.

• Modify Template:

In this attack, the attacker compromises the security of the database of templates. The attacker can add fake templates, modify or delete the existing templates.

• Intercept the Channel:

This attack is similar to the attack Replay Old Data. In this attack, the attacker sniffs the communication channel between the database and matcher to steal and then replay or alter the data.

• Override Final Decision:

In this attack, the attacker sniffs the communication channel between the matcher and the application to replay or alter the data.

6. Cryptography in e-passports

6.1. The ICAO specification

The ICAO standards has specified cryptographic measures and control technics to be implemented in e-passport [5]. It presents one mandatory cryptographic feature and five optional advanced security methods.

6.2. Passive Authentication (PA)

The ICAO specifications have both mandatory and optional features for security and authentication. The mandatory features provide only a basic level of security and do not prevent copying of data stored on the contactless IC. The integrity of the data stored in the LDS and Security Object Descriptor (SO_D) is verified and authenticated by PA.
Deficiencies
- Does not prevent an exact copy or chip substitution
- Does not prevent unauthorized access
- Does not prevent skimming

6.3. Active Authentication (AA)

AA is an optional security feature that depends on public key cryptography to protect the chip against modification or cloning. It uses challenge-response protocol to prevent copying the SOI and proves that data has been read from the authentic chip. Further, it proves that chip has not been substituted.

Deficiencies
- Adds (minor) complexity
- Does not prevent an exact copy of contactless IC and conventional document

6.4. Basic Access Control (BAC)

ICAO recommends BAC as an optional feature against data skimming and misuse. A chip that is protected by BAC mechanism prevents eavesdropping on the communication between MRTD and inspection system. The protocol uses two secret keys \([K_{ENC}, K_{MAC}]\) that are stored in e-passport chip. The reader retrieves the secret keys by optically scanning the data presented in MRZ. Finally, both the reader and tag generate session key to encrypt the communication between them.

Deficiencies
- Does not prevent an exact copy or chip substitution (requires also copying of the conventional document)
- Adds complexity
- Requires processor-ICs

6.5. Extended Access Control (EAC)

It adds functionality to check the authenticity of the reader (terminal authentication) and chip (chip authentication) to prevent an unauthorized access to additional biometrics. This is typically used to protect the iris scan and fingerprints.

Deficiencies
- Requires additional key management
- Does not prevent an exact copy or chip substitution (requires also copying of the conventional document)
• Adds complexity
• Requires processor-ICs

6.6. Cryptography Threats

The recommended minimal key lengths have been chosen so that breaking those keys requires a certain effort, independent of the chosen signature algorithm.

<table>
<thead>
<tr>
<th>Type of Key</th>
<th>Level of Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Signing CA</td>
<td>128 bits</td>
</tr>
<tr>
<td>Document Signer</td>
<td>112 bits</td>
</tr>
<tr>
<td>Active Authentication</td>
<td>80 bits</td>
</tr>
</tbody>
</table>

Table 1: Cryptographic Threats

7. Discussions on Security and privacy risks with the E-Passport

The ICAO standard allows EAC, an additional security access mechanism to meet data protection requirements and to enhance the privacy of additional biometric data (such as fingerprints and iris identifiers). Addition of metallic shield (a Faraday cage) to cover e-Passport to prevent skimming and BAC to prevent unauthorized readers from accessing the chip was implemented. These properties will make attacker more difficult to modify the stolen or lost passports as the new name and information would differ from the information on the RFID tag. All e-passports issued must follow the common ICAO standard. However, countries implement e-passport programs according to their specific policies and are free to implement different options specified in the standard. Because of this, there are some differences on implementation of e-passports among several countries even though they all confirm to the ICAO specification. The US State Department specified that the new US passports would increase the available memory from 32 kilobytes to 64 kilobytes apparently to reserve for some more biometric characteristics. The State Department also made compulsory rule for using the metallic layer to cover the passport in order to prevent the reader to read the tag. The idea of using the metallic shield is a good concept but it does not provide a complete solution. Since, passports are used for personal identification all over the world, one needs to open it which makes the exposition of RFID. For example, when one needs to reserve the hotel, the passport must be opened and allowed to be photocopied.
Multimodal Biometric features are useful and widely used for authentication process, but misuse of these features can make severe loss of vital private information. Several technologies are implemented in order to prevent from security threats, among them Biometrics is proved to be more secure than others.

8. Recommendation

- The proposed idea regarding e-visa information on e-passport [16] may not be feasible. Generally, the passport is valid for 5-10 years and if the visa information is stored in the same chip with passport information then frequent writing of visa can have some consequences like data collision and durability of the chip. One solution can be the use of a separate RFID tag for visa stamps. Even though, tag collision may occur since two RFID tags reside in the same area but still this is feasible because data can be read in a very short time.

- Human beings can be represented as a digital identity based on their unique biological characteristics (Biometrics) such as face, iris, and fingerprint. The deployment of Biometrics technology is to improve the privacy and security aspects during authorization process by creating a digital identity for an individual. If an attacker can intercept the biometric system and successfully retrieve the encoded data then the data are lost forever until and unless the replacement of new fingers (in case of fingerprint). More advanced cryptographic technology must be implemented in order to enhance the security and privacy issues.

- The mandatory and optional security requirements defined by ICAO in the latest documentation needs to be reviewed. There is no uniformity among the countries in using biometric and protocols (security schemes). Hence, if global standards are not maintained then the possible security features and the importance of interoperability cannot be adapted in full fledge.

- RFID is an enabling technology commonly used in various applications and the best known application is e-passport. Most of the developed countries are already using e-passports and many countries are on issuing process. There are still many issues concerned with privacy and security of RFID which need to be addressed. If we do not focus to solve and continue to issue only the e-passport then the world has to bear huge financial loss in the days to come like now the world is investing against the threats/viruses especially in internet technology.
9. Conclusion

The latest privacy and security issues that evolved in the field of e-passport is a challenging task and fundamental modification are needed to be implemented on both the ICAO and EU security specifications. E-passports contain entirely the private information, so protection of data is extremely essential. Authenticity, confidentiality and data integrity are the most crucial factors and can be maintained by using cryptography.

Biometric is quite new concept and is stepping further evolution every year with new vision and system improvement. The deployment of e-passport is an important step in passport technology that provided important evidence and opened the door to build more secure and identification platform where the exchange of private data will be better protected in the days to come.

Hence the emerging technology like e-passports facilitates the users in one hand but there are still some big problems that need to be addressed and evaluated extensively. RFID and Biometrics technology has huge impacts on privacy and security issues of an individual; hence the government must not ignore and start to work on it.
10. References

