An Analysis of Security Weaknesses in the Evolution of RFID Enabled Passport

Eyad Abdullah Bogari, Pavol Zavarsky, Dale Lindskog, Ron Ruhl
Information Systems Security Management
Concordia University College of Alberta
7128 Ada Boulevard, Edmonton, Alberta, Canada T5B 4E4
eyad.bogari@gmail.com, {pavol.zavarsky, dale.lindskog, ron.ruhl}@concordia.ab.ca

Abstract-Since the introduction of Radio Frequency Identification (RFID) Enabled Passports, the system have been plagued with various vulnerability issues that prove to compromise the E-passport security. To date, three generations of E-passports have been introduced by the International Civil Aviation Organization (ICAO) and the European Union (EU). The first two generations of E-passports are being issued worldwide. This paper presents the evolution of these passports over the years to develop taxonomy of the weaknesses and to serve as a reference point detailing security vulnerabilities linked to the RFID E-passport features in the first and second E-passport generations. The findings can also assist in profiling possible attack vectors on the existing RFID enabled passports and in developing comprehensive RFID E-passport risk mitigation strategies. To illustrate the importance of a comprehensive risk strategy when using RFID E-passport, the attack process modeling method is used to highlight the possible attacks and weaknesses which could result from not using one or more security features.

Keywords: RFID, E-passport security features, E-passport vulnerabilities, ICAO, PKI

I. INTRODUCTION

Radio Frequency Identification (RFID) is an automatic identification technology that transmits data through the use of wireless communication using radio waves. The RFID technology was first used in World War II (WWII) for identification, friend or foe (IFF) systems. The RFID has been used for the purposes of identifying an object or a person. The transmission of data is carried out between a reader and an electronic chip attached to an object or a person. An RFID system for Enabled Passport (E-passport) consists of a chip, a reader, an antenna, and a Public Key Infrastructure (PKI) (see Section 1.1). There are three types of RFID chips, namely active, passive and semi-passive. Passive chips differ from active for getting energized by reader radio waves. Passive chips are battery-less and they follow ISO/IEC 14443 standards that specifies two alternative types of Integrated Chip (IC) [23]. The specifications allow either type to be used in the presence of an RFID reader capable of operating in both systems. Issuing countries are consequently encouraged to consider possible future requirements when specifying IC capacity, especially where multiple biometrics may be used which similar to the second generation. The E-passport operates at radio frequency of 13.56MHz.

1.1 E-passport: Infrastructure Components

Countries around the globe are shifting to the new RFID Enabled passport modules. The E-passport contains an RFID chip which holds sensitive information: passport number, issue and expiry date, issuing country, full name, gender, nationality, date of birth, document type, digital picture of the passport holder, and fingerprint or iris scans. The same information is present on the photo page of the passport. The switch to E-passport requires the use of Public Key Infrastructure (PKI) to prove authenticity and integrity of the Machine Readable Travel Documents (MRTDs) [29]. The PKI is built to ensure that travelers privacy is protected. Furthermore, the data stored in the chip is digitally signed. Both in the first and the second generation of E-passports, the digitally signed data consists of sixteen Data Groups (DGs). The DGs hold sensitive personal data, digitized biometric measurements and Machine Readable Zone (MRZ). On the other hand, issuing countries need to verify authenticity of the data stored in the chip and no one has tampered it. While using public key cryptography to digitally sign the sensitive data stored on the chip protects the data, it cannot prevent an attacker from copying the data from the chip. This is one of the privacy concerns that have been raised by researchers and experts.

The ICAO proposes using the PKI architecture within the highest hierarchy level for each country. Each country has an independent PKI design and architecture. Each country also needs to implement and enforce proper security policies. According to the ICAO, there are two key elements that should be in the PKI architecture: 1) the Country Signing Certificate Authorities (CSCA) and 2) Document Signing Certificate Authorities (DSCA). In addition, the two key elements work with the Certificate Revocation Lists (CRLs) at Inspection System (IS) points. An IS point, which is a computer-based system, has an MRZ reader capable of reading the Document Basic Access Keys (K_{ENC} and K_{MAC}). K_{ENC} is a key for message encryption while K_{MAC} is a key for message authentication. However, each IS point must have PKI key information such as issuing CSCA stored in the system. Each country is responsible for maintaining the information updated in the Public Key Directory (PKD). In addition, a key pair is generated for Active Authentication (AA) mechanism: a public key (KPu_{AA}) and a private key (KPr_{AA}). The public key is issued by the CSCA and the private key is created and stored in the chip. However, the

private key once generated will be stored in the E-passport until the passport expires.

1.2 Our Contribution

We expect that the presented review on the security features and vulnerabilities can serve as a reference point detailing security vulnerabilities linked to the RFID E-passport features in the first two E-passport generations. The presented survey can also be used in threat analysis and assist in profiling possible attack vectors on the RFID enabled passports. The findings presented in the paper can be useful in developing a comprehensive risk management strategy in the implementation and use of the RFID E-passports. Therefore, the attack process modeling method will be used to assist in profiling the possible attacks and weaknesses which could result from not using one or more E-passport security features.

The structure of this paper is as follows: Section II discuss an overview of the evolution of security features of the RFID enabled passports. Taxonomy of the security vulnerabilities are developed in Section III and Section IV is an illustration of the possible attacks and weaknesses using the attack process modeling method.

II. OVERVIEW OF RFID E-PASSPORT GENERATIONS

The ICAO and EU guidelines specify that the face of the passport holder should be used as a mandatory biometric along with the sensitive personal information. The guidelines also specify that iris and fingerprint recognition are two optional features that may be used by issuing countries for additional implementation of access controls. These biometric features, together with the data stored in the chip, are required to be digitally signed.

Countries following the ICAO and/or EU standards are required to use Passive Authentication (PA). According to the German Federal Office for Information Security (BSI), the Active Authentication (AA), Basic Access Control (BAC), and Extended Access Control (EAC) are mandatory protocols for E-passports of the second generation [8]. Other non-EU countries have the choice of using optional features introduced by the BSI. The optional features permit issuing countries to enforce additional data security.

Table 1 shows the ICAO and the EU E-passport specifications. Both the ICAO and EU specifications mandate the use of face biometrics. The ICAO guidelines specify three cryptographic protocols, one is mandatory and two of which are optional. In the first generation of E-passports, the PA is mandatory and AA and BAC are optional. The EU specifications also require the use of PA in the first generation of E-passports. Under the European Union umbrella, the BSI introduced second generation of E-passports with the Extended Access Control. The EAC in the second generation E-passports consists of the Chip Authentication (CA) v1 and Terminal Authentication (TA) v1, along with the PA and BAC. The second generation is being implemented and used by the EU countries.

Table 1: ICAO and EU E-passport Specifications

Mechanism	Type	Organization
First Generation		
Passive Authentication	Mandatory	ICAO & EU
Active Authentication	Optional Mandatory	ICAO EU
Basic Access Control	Optional Mandatory	ICAO EU
Biometric: Face	Mandatory	ICAO & EU
Second Generation		
Passive Authentication	Mandatory	ICAO & EU
Basic Access Control	Mandatory	ICAO & EU
Chip Authentication v1	Recommended Mandatory	ICAO EU
Terminal Authentication v1	Recommended Mandatory	ICAO EU
Biometric: Face	Mandatory	ICAO & EU
Biometric: Fingerprint	Optional Mandatory	ICAO EU
Biometric: Iris print	Optional	ICAO

A. First Generation E-passport Security Features

Passive Authentication (PA) Mechanism

In the first generation of the RFID E-passports, the ICAO guidelines define PA as the only mandatory mechanism. The main purpose of PA is to allow a reader to verify the integrity of the data stored in the chip has not been altered. This enables the Inspection System of the E-passport PKI to identify any changes that has been made to the data. In addition, ICAO specification suggest that the data stored on the chip is organized in a Logical Data Structure (LDS) and that it contains cryptographic keys for BAC, private key used in AA, and sixteen Data Groups (DGs). The DGs are digitally signed by the appropriate issuing state and each DG is hashed to form a Document Security Object (SO_D). Further, the PA requires two separate Certification Authorities: The Document Signer (DS) and Country Signer Certification Authority (CSCA). The Document Signer Certificates (C_{DS}) are signed by the CSCA. The DS is located in the passport personalization machine and generates the Document Individual Security Object SO_D, see [32] for details. Following this, the Inspection System IS which contains the Document Signer Public Key (KPu_{DS}) locates the certificate and verifies the authenticity of the digital signature using the Country Signing Certificate Authority Public Key (KPu_{CSCA}). The RFID reader then computes the hash of each data set and compares it with the data stored in the SO_D. If there is a match, it can be established that the data on the chip was not manipulated [36]. However, the PA mechanism does not verify that the holder of the E-passport is the owner of the passport. The ICAO made it clear in [47] that the PA does not prevent copying of the chip content or chip substitution. Therefore, the confidentiality of the data contained in the MRZ can be compromised and additional security features are required.

Basic Access Control (BAC) Mechanism

The BAC is one of two optional security features, but recommended security features (see Table 1) specified in the ICAO standard for the first generation E-passports. While the BAC is optional in the ICAO standard, the EU specifications mandate the use of BAC for all E-passports of the EU countries for enhanced data protection. Deployment of the BAC ensures that the chip can be physically read by authorized RFID E-passport readers. The BAC is used between the RFID reader and the E-passport chip for establishment of session keys K_{ENC} and K_{MAC} for Message Authentication Code (MAC). The K_{ENC} and K_{MAC} are derived from the MRZ data (the passport number, the date of birth and the date of expiry). The BAC deploys symmetric cryptography and generates corresponding encryption and authentication keys from passport information that is visible in the physical passport document, see [33]. The information stored in the MRZ has a significant role in the derivation of the BAC keys, specifically the information in the bottom two lines printed on the photograph page of the passport [33].

The Optical Character Recognition (OCR) reader reads the MRZ data of the above three items, calculates a DES or 3DES key as appropriate and then the RFID reader reads the content of the E-passport chip using the calculated key. The process of exchanging the key pair comes with a challenge response mechanism which proves the existence of a key pair derived from the collected information of the MRZ. The session keys ensure confidentiality and integrity of the transmission of the data between the RFID reader and the chip. If authentication is successful, the E-passport chip releases its data, otherwise the reader is considered as unauthorized and the passport refuses the read access [45]. Upon successful verification, a Secure Messaging (SM) occurs which is an encrypted and authenticated channel between E-passport chip and IS. Secure Messaging can be set up by the BAC, CA, or Password Authenticated Connection Establishment (PACE). The BSI has indicated in [8] that the provided security level depends on the mechanism used to set up the SM. The weakness of the BAC rests in the key derivation which comes from the passport number, the date of birth, and the expiry date.

Active Authentication (AA) Mechanism

The AA (also known as an anti-cloning mechanism) is another optional security feature specified in the ICAO's guidelines. On the other hand, the EU specifications mandate the use of AA mechanism for additional data protection (see Table 1). The AA was designed to protect E-passports from cloning or chip substitution and deploys asymmetric cryptography. The AA is part of the sixteen Data Groups (DGs) organized in the LDS and contains key pair: public and private. The public key KPu_{AA} is stored as part of the LDS specifically in the DG-15 and a hash of the public key KPu_{AA} is stored in the Document Security Object SO_D. Moreover, the private key KPr_{AA} is stored in the contactless chip's secure memory throughout the life of the passport. Both public and private keys work in a mutual authentication process to prove that no alteration or cloning was involved. The AA makes it possible to verify identity and authenticity of the chip itself and prevent passport forgery using a false chip, see [36]. Yet, the ICAO indicated in [47] that while the chip substitution might be difficult, but not impossible for attackers.

B. Second Generation E-passport Security Features

The Extended Access Control (EAC) is a mandatory security mechanism, (see also Table 1), introduced by the EU specifications for the second generation E-passports. On the other hand, the ICAO defines the EAC as an optional security feature and gives issuing countries the choice in the implementation of E-passport security. The EAC is needed for additional security and access controls, such as fingerprint recognition for border security. The EAC consists of the Chip Authentication (CA) v1 and Terminal Authentication (TA) v1. The CA works in the same way as AA, which proves the authenticity of the chip. The TA verifies to the chip that the terminal is permitted to access the data on the chip [21]. The EAC is similar to the BAC, but the difference is that the EAC uses Document Extended Access key instead of the Document Basic Access keys K_{ENC} and K_{MAC}. According to the ICAO specifications [47], the Document Extended Access key may consist either of symmetric or asymmetric key pair.

Chip Authentication (CA) Mechanism v1

The CA v1 is a mandatory protocol set by the EU for the second generation E-passport (see also Table 1). The CA v1 is a replacement of the AA and its purpose is to detect cloned E-passports. If CA is performed successfully, it establishes a new pair of encryption and MAC keys to replace the BAC derived session keys and enable secure messaging, see [36]. After successful BAC, the CA v1 involves the Diffie-Hellman (DH) agreement followed by the PA and TA. In addition, the CA v1 uses key pair: public and private. The public key (PK_{PICC}) is in the DG-14 and the private key (SK_{PICC}) is stored in the chip memory. The BSI explains the CA v1 mechanism as an ephemeral-static DH key agreement protocol that provides secure communication and independent authentication of the Machine Readable Travel Document (MRTD) chip, see [2]. The ephemeral-static DH key agreement means that the key pair lasts for short period of time and is used once. The CA v1 provides implicit authentication of both the chip itself and the stored data by performing SM using the new session keys [8]. The CA v1 is vulnerable to attacks such as eavesdropping and side channel attacks, see Section III.B for more details.

Terminal Authentication (TA) Mechanism v1

The TA v1 is also a mandatory protocol set by the EU specifications for the second generation E-passports (see Table 1). It is used to prove to the E-passport chip that the terminal is permitted to access sensitive data on the chip. According to the BSI technical guidelines [8], such terminal is equipped with at least one Terminal Certificate (TC), encoding the terminal's public key (PK_{PCD}) and access rights, and the corresponding private key (SK_{PCD}). After the terminal has proven knowledge of the private key SK_{PCD}, the MRTD chip grants the terminal access to sensitive data as indicated in the TC. The terminal certificate is issued by the Country Verifying Certification authority

(CVCA) for Document Verifier (DV). The CVCA permits any DV access to the sensitive data on the E-passport chip. Similarly, the PA uses a certificate issued by the CSCA for any DS's (see section A). According to [8] the CSCA and the CVCA may be combined into a single entity called Country Certification Authority. The TA v1 can only be used in combination with CA v1. In addition, the specifications of the EU also mandate the use of a secondary biometric for further border access control security. The TA v1 occurs after the CA v1. Therefore, the TA v1 authenticates an ephemeral public key chosen by the terminal that was or will be used to set up Secure Messaging with the CA, see [8]. Moreover, there are three types of terminals that can be used for further details checks: 1) Inspection Systems, 2) Authentication Terminals, or 3) Signature Terminals, see [2]. Yet, the TA v1 occurs after the CA v1, which is a security weakness. An attacker can gain access to the CA v1 and get sensitive information.

III. SURVEY OF E-PASSAPORT VULNERABILITIES

Governments around the globe are issuing the RFID E-passports to their citizens. Thus, sensitive data are stored within the embedded chip and the holders of the passports need assurance that the employed security protects their sensitive data. However, the E-passports may not be able to guarantee this since inherent security vulnerabilities exist from the very first generation of the E-passport. There are threats related to reading the information on the chip without the holder‘s consent, such as clandestine scanning, clandestine tracking, skimming and cloning [45].

In this section we are reviewing the vulnerabilities associated with the use of the first and second RFID E-passport generations. The review results are presented in tables listing possible attacks and weaknesses in each of the generations. Furthermore, the tables list both technical and non-technical vulnerabilities for each generation. Non-technical vulnerabilities, such as bribing an insider, blackmailing, threatening, or impersonating are all types of vulnerabilities that exist in the two E-passport generations. In the following sections we first discuss the first generation vulnerabilities, followed by the description of vulnerabilities in the second generation.

A. First Generation E-passport Security Vulnerabilities

The security of the RFID E-passports is an area that has been heavily researched and a wealth of information is available to analyze weaknesses, threats and risks associated with the use of E-passports in the different generations. The wealth of information has allowed us to develop taxonomy of identified vulnerabilities throughout the two generations of RFID E-passports. Table 2 shows a summary of the vulnerabilities including possible attacks and weaknesses that could occur in the first generation of the RFID E-passport.

The first generation of E-passports has some common vulnerabilities that can occur in the PA, AA, and in the BAC. In the first generation, the Man-in-the-Middle (MITM) attacks are hard to defend even with encryption [19], [44]. Also, as shown in [44], an attacker can potentially impersonate the card of a nearby person to an official RFID reader just by relaying messages to and from that nearby person's card. Furthermore, [15] illustrates that replay attacks can occur and an attacker can listen to the identification of a certain chip and can forward the same message to the reader behaving like the original chip. Rotter describes in [42] how relay attacks occur between a legitimate RFID reader and an illegitimate chip and between a legitimate chip and an illegitimate reader. Also, an attacker can use a jammer or blocker for a Denial-of-Service attack paralyzing the communication channel between RFID readers and E-passport chips [42].

Table 2: First Generation E-passport Vulnerabilities and Possible Attacks

First Generation E-passport Vulnerabilities and Possible Attacks		
Passive Authentication	Active Authentication	Basic Access Control
Weaknesses/Flaws		
Biometric and Data leak 21,36	Biometric and Data leak 21,36	Biometric and Data leak 21,36
Certificate Authority key 43	No unique key pair generation 2	Low Key Entropy 2,5,9,11,21,26,33,35,36,38,38,40,41
Altering chip and biometric data 2,27		Calculation of the BAC keys 4,38
Attacks		
Bribing 27	Bribing 27	Bribing 27
Man in the middle 19,44	Man in the middle 19,44	Man in the middle 19,44
Replay 15,10	Replay 15,10	Replay 15,52
Relay 42	Relay 19,42	Relay 42
Jamming and Blocking 42	Jamming and Blocking 42	Jamming and Blocking 42
Cloning 2,3,4,7,13,25, 26,29,31,32,34,36,38,42,45,47	Cloning 10	Brute Force 40,41
Skimming 2,4,5,14,17, 26,27,29,36,37,38,40,45	Side Channel (power and timing) 20,36	Side Channel (power and timing) 20,36
Tracking 2,11,15,21,26, 37,38,42	Tracking 26	Cipher-text 52
Eavesdropping 3,4,11, 15,17,21,26,27,29,32,33,37,38,40,41,42,45	Grandmaster Chess 45,47	Plain-text 52
Spoofing 3		
Terrorist act (bomb) 21,26		

3.1.1 Passive Authentication (PA) Vulnerabilities

The PA does not verify that the holder of the E-passport is really the owner of the E-passport and does not prevent copying of data. This introduces the possibility of cloning and other types of attacks. Cloning is copying or duplicating data of a chip found in the MRZ to another chip or system without the knowledge of the passport holder. This type of attack occurs to the mandatory feature of PA. Researchers in [2]-[4], [7], [13], [25], [26], [29], [31], [32], [34], [36], [38], [42], [45], [47] have identified that cloning is a serious vulnerability and successful attacks can compromise confidentiality of the MRZ E-passport chip data. Grunwald demonstrated in [31] that the first generation passports designed using the ICAO standard can be easily cloned. Additionally, as shown in [32], copying of data is possible by performing the BAC, and then writing the data (including the

SO_D) to a new RFID chip from which personalization keys are known. The result of the cloning is that the data has not been changed and therefore even the Passive Authentication will not recognize the counterfeit, see [32]. The simplicity of the attack has been shown in [50] using a Motorola RFID reader and an antenna attached to a computer.

Beek demonstrated in [7] the possibility to alter and clone the first and second generation of E-passport chips. He altered the image embedded within the E-passport and demonstrated that then the altered chips were passed as genuine. According to [13], the Israeli secret service Mossad cloned 1000 British E-passports of the first generation, and the airline staff working for Mossad may have copied the E-passports of Britons flying to Israel. Twelve first generation E-passports were used in the assassination of senior Hamas figure Mahmoud al-Mabhouh in Dubai after the passports were cloned at different airports while the British nationals were on their way to Israel [13]. The cloning pose a threat of information leakage (data and biometrics) contained in the E-passport chip. Furthermore, researchers in [2], [21], [27], [36] illustrated that biometric leak and alteration of biometric data are possible. However, the ICAO indicated that the optional feature of AA in the first generation of E-passports detects cloned chips if implemented by the issuing country along with the PA. Moreover, spoofing represents a variant of cloning that does not physically replicate the RFID chip by using special devices with increased functionality, see [3].

Eavesdropping, intercepting or monitoring the communication between an E-passport chip to a reader and vice versa, is also possible in the first generation of E-passports. The eavesdropping can result in stolen sensitive information, such as E-passports biometrics, personal information or cryptography information. For example, in the first generation, an eavesdropper can use an illegitimate RFID reader to eavesdrop on channel between an E-passport chip and RFID reader. Researchers in [3], [4], [11], [15], [17], [21], [26], [27], [29], [32], [33], [37], [38], [40]-[42], [45] emphasize that eavesdropping can occur without the E-passport holder knowledge. Eavesdropping also may occur to facilitate other types of attacks.

Moreover, the RFID E-passport chips transmit radio waves broadcasting information once the E-passport is either partially or fully open which makes the E-passports prone to skimming. The RF also allows an attacker to track a person once the victim opens the passport. According to the ICAO, ten meters (33 ft) is enough for an attacker to skim the information when the E-passport is open or partially open. Furthermore, skimming is a reading of the content of the data in the MRZ without being detected. An attacker can use an illegitimate reader to skim the data of the MRZ. Researchers in [2], [4]-[5], [14], [17], [26], [27], [29], [36]-[38], [40], [45] pinpoint that skimming is a vulnerability to the E-passport holder confidentiality.

Additionally, as shown in [2], [11], [15], [21], [26], [37], [38], [42], the RFID E-passport allows a person to be tracked. For example, an attacker can gain access to the sensitive data including the Unique Identifier (UID). The UID helps an attacker to track an individual using either static or random identifier. The type of the UID, static or random, is determined by the E-passport issuing country. Researchers in [21], [26] illustrated that the RFID-bombs is a type of an attack. An attacker could trigger the RFID bomb based on the UID.

Schneier in [43] gave details on how Certificate Authorities might be vulnerable and an attacker may get access to the Certificate Authority's key by bribing an insider or to gain access to the key due to a human error. An attacker can use various social engineering attacks, including blackmailing, and threatening an insider who works for the passport issuing government agency to bypass the E-passport security [17].

3.1.2 Basic Access Control (BAC) Vulnerabilities

In the BAC, there is a way of figuring out the key by knowing the passport number, the date of birth, and the date of expiry. The MRZ information which contains three elements: the passport number, the date of birth, and the date of expiry including their respective check digits can be used by attackers to derive the access key seed. In fact, the access key seed can be easily calculated. As shown in [40], [41], due to the low entropy of 56 bit keys, the BAC is vulnerable to brute-force attacks. [21], [29], [45] show that guessing the key based on calculations would be sufficient in knowing the access keys. The actual entropy mainly depends on the type of the document number. For example, for ten-year valid travel document the maximum strength of the keys is approximately 56 bit for a numeric document number and 73 bit for an alphanumeric document number, see [46] for more details.

As shown in [5], on-line and off-line attacks can be used to get the BAC keys. For example, an off-line attack can be conducted by eavesdropping on a legitimate communication and that the on-line attacks by skimming. Then, after the eavesdropping or skimming, the attacker can use brute-force attack to get the BAC keys.

As shown in [52], an eavesdropper might be able to collect information about several runs of the protocol and perform a cipher-text attack with known partial plain-text attack to obtain the session key and/or MRZ information that is necessary to create K_{ENC} and K_{MAC}. Any loss of K_{ENC} or K_{MAC} keys makes the E-passport vulnerable to skimming and snooping attacks.

3.1.3 Active Authentication (AA) Vulnerabilities

As shown in Table 1, the ICAO indicates that the AA is an optional feature allowing issuing countries to implement the security feature. The AA increases the cryptographic capabilities and this is an advantage over the Passive Authentication because the AA comes with faster processing times and works in conjunction with the BAC. The AA uses the same key pair for every authentication session, no temporal keys for every new session and no external or terminal authentication are performed, see [8]. While risks of cloning are mitigated by the AA, side channel attacks (power and timing attacks) on E-passport chips can be used to obtain the active authentication private key, see [36]. As shown in [20], power and timing attacks assist in obtaining the AA private key. Moreover, as shown in [10], the

file indicating features of the E-passport is not included in the SO_D and thus can be modified unnoticed. After removing the Active Authentication, the terminal will continue without executing the AA procedure, so the chip could be cloned even if the original passport was employing AA [10].

As shown in [26], an individual can be tracked even if the data on the chip cannot be read. They also showed that the AA feature enables tracking when used with the RSA or Rabin-Williams signatures. Sheetal and the ICAO Doc 9303 [45], [47] show that the Grandmaster Chess attack is similar to cryptographic tunneling attack in which the Inspection System does not know that a remote chip was authenticated instead of a presented one. Furthermore, [19], [42] explained how relay attacks on the AA could be dangerous. An attacker in the relay attack creates a channel between a legitimate reader and illegitimate chip and vice versa.

B. Second Generation E-passport Security Vulnerabilities

The second generation of E-passports was implemented to help overcome the weaknesses of the first generation. The security of the second generation of E-passports depends on the Basic Access Control to provide protection to E-passport chip data. Table 3 shows a summary of the vulnerabilities associated with the use of Chip Authentication v1 and Terminal Authentication v1. Furthermore, attackers could use illegal non-technical ways to get sensitive information from the passport holder or by bribing, blackmailing, or threatening a government official.

3.2.1 Chip Authentication (CA) v1 Vulnerabilities

The second generation CA was introduced to avoid the problems associated with the AA and to avoid side channel attacks by implementation of secondary cloned chip detection algorithm. However, the CA v1 does not successfully mitigate side channel attacks [6]. In addition, an attacker could eavesdrop on a legitimate communication between a chip and a reader using an illegitimate reader. For example, Chothia and Smirnov [11] conducted an experiment to trace an E-passport by eavesdropping on a legitimate session and by recording the encrypted message containing the nonce. Their experiment demonstrated that rejected replayed messages of an incorrect nonce are different from the replayed messages of failed authentication checks. The CA requires high-end processors for performing the DH key exchange, which can be viewed as a weakness [45].

As shown in [52], CA is vulnerable to the Grandmaster Chess attack to which the first generation E-passport is also vulnerable to (see Section A.3.1.3). The [52] also shows that the BAC does not provide authentication. Therefore, the chip establishes a session key even though it is not sure if the Inspection System is genuine. The EAC is also vulnerable to jamming and blocking attacks. For example, an attacker could use a jammer or a blocker to jam communication between the RFID reader and the E-passport chip and to perform Denial of Service DoS attack [42].

Moreover, dependence on the BAC results in the first generation low key entropy weakness (see Section A.3.1.2) especially if the E-passport numbers are sequentially produced [52]. For example, an attacker can exploit the weakness of the keying scheme to recover the data exchanged between the terminal and the E-passport.

Table 3: Second Generation E-passport Vulnerabilities and Possible Attacks

Second Generation E-passport Vulnerabilities and Possible Attacks	
Chip Authentication v1	Terminal Authentication v1
Weaknesses/Flaws	
Altering chip and biometric data 2,27	Altering chip and biometric data 2,27
Dependence on the BAC keys 37,52	Stolen Terminal 21
Low-end processors for DH keys 45	Once Valid Readers (expired certificate) 36
Attacks	
Bribing 27	Bribing 27
Tracking 3,4,12,24,29,39,41,43	Tracking 3,4,12,24,29,39,41,43
Jamming and Blocking 42	Jamming and Blocking 42
Side Channel attack 6	Denial of Service 15,36,37,51,52
Eavesdropping 3,4,11,15,17,21,26,27, 29,32,33,37,38,40,41,42,45	
Grandmaster Chess 52	
Replay attack15,10	

In addition, second generation E-passports are vulnerable to attacks by once validated RFID readers. As shown in [36], it is possible for a reader with expired certificate to read an E-passport chip even if the date on the chip was not updated. This is due to the passive nature of the chip and because it does not use the time information. Furthermore, each country is responsible for the implementation and design of the PKI and E-passport chips and each country has its own unique Answer to Reset (ATR) value [31]. The ATR value can be used to track an individual. Researchers [36], [37] demonstrated that a person can be also tracked using the CA. The chip sends its identification details (public key) during the CA even before it has authenticated the IS. Therefore, this mechanism allows tracking, as an attacker is not required to authenticate to an E-passport before obtaining details from the E-passport [37].

3.2.2 Terminal Authentication (TA) v1 Vulnerabilities

In the second generation, the TA is performed after the CA. The TA is vulnerable to the DoS attack [15], [36], [37], [51], [52]. Nithyanand showed in [36] that an attacker could flood the chip with invalid certificates using the RFID reader. Due to the limited memory on the chip, this can cause the chip to stop functioning. Also, as shown in [36], an attacker can use a jammer to jam the RFID signal or block the signal and disrupt the communication channel between the RFID reader and E-passport chip [42]. The TA is vulnerable to once valid readers which allow a reader to read an expired certificate. This is caused by the passive nature of the chip and can happen when the chip was not updated for a while like in cases of infrequent travelers [36]. Moreover, Hoepman and his colleagues discussed how stolen terminals cannot be revoked. In addition, an attacker

could alter chip biometric data by using wax fingers or face masks [2], [27].

IV. Examples of E-Passport Security Analysis Using Attack Process Modleing

Attack trees provide a way to systematically analyze ways how vulnerabilities in a system or its components can be exploited to compromise security of the system. The attack tree threat analysis has proved to be useful in developing controls mitigating or eliminating possible attacks. In the attack process modeling, the attacks are divided into sequences or attack steps to be completed to achieve the attack goals. The following two examples illustrate the E-passport security analysis using the process modeling.

Example 1: Modeling of exploitation of vulnerabilities in E-passport security features for the man-in-the-middle attacks.

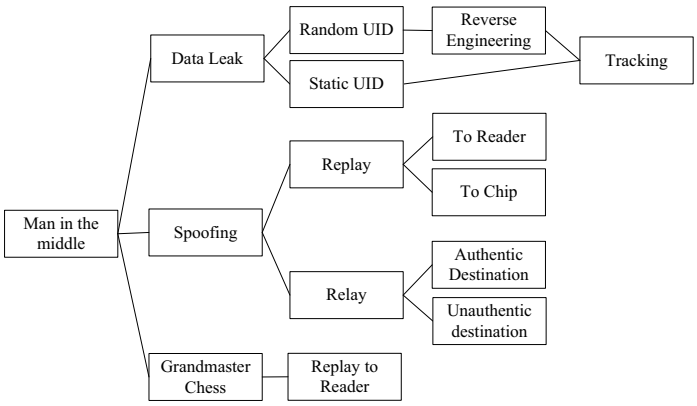

Fig 1: Man-in-the-Middle Attack Modeling

The data leak, spoofing and data origin authentication (Grandmaster Chess) vulnerabilities make E-passports vulnerable to the man-in-the-middle attacks. The attacks are modeled in Fig.1. The figure shows relaying of data to authentic and unauthentic spoofed destinations, replaying to chip and/or reader, and tracking based on the data leak of the UID.

Example 2: Modeling of attack sequences needed to exploit Basic Access Control (BAC) low key entropy vulnerability.

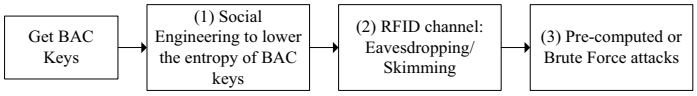

Fig 2: BAC Attack Process Modeling

The BAC security feature of E-passports of the first and second generations was introduced in Section II and the limitations of the BAC in securing E-passports were reviewed in Section III. The BAC keys are derived from 1) the passport number, 2) the date of birth, and 3) the date of expiry. The information in the E-passports both in human-readable and machine-readable (in the MRZ) are on the photo page of the passport. Social engineering attacks enable harvesting of the passport holder information that is required for the generation of the BAC access keys K_{ENC} and K_{MAC}. The passport holder information effectively reduces the keys' entropy and facilitates attacks on the cryptographic keys. The entropy of the key is at most 56 bits in the ICAO passports and can be reduced because of the key generation scheme. Low entropy makes the BAC keys vulnerable to attacks. Eavesdropping on the legitimate RFID channel can be combined both with pre-computed rainbow table attacks and brute force attacks on the BAC access keys. Fig 2 illustrates the steps that attackers can use to get the BAC keys. The figure also suggests possible ways to defend against the attack. While elimination of successful social engineering attacks on the information available in human-readable form on the photo page of E-passports is unlikely, the online and off-line RFID eavesdropping and skimming attacks can be reduced by physical, technical, and operational controls.

CONCLUSION

In this paper we presented a review of security features and vulnerabilities across two generations of the RFID enabled passports. The survey shows that some of the vulnerabilities of the first generation E-passports have been eliminated by the security features of the second generation. The security features include Chip Authentication and Terminal Authentication mechanisms. Yet, there are countries that are still using the first generation E-passports. Moreover, as shown in the paper, there are both technical and non-technical vulnerabilities that are present in the first and second E-passport generations. The presented review can serve as a reference point detailing the associated security vulnerabilities linked to the RFID E-passport features in the existing passport generations. The presented survey also used the attack process modeling methodology to assist in profiling possible attack vectors on the RFID enabled passports. The findings presented in the paper can be useful in developing comprehensive risk management strategies in the implementation and use of the RFID E-passports.

ACKNOWLEDGEMENT

The first author would like to thank his research advisors Dr. Pavol Zavarsky, Dr. Dale Lindskog and Ron Ruhl, for their encouragement, guidance and support in accomplishing this research. The author also would like to acknowledge the King Abdullah Scholarship Program for personal funding. Also, the author is grateful to David Edwards for his motivation and knowledge. Lastly, special thanks go to my wife Yara and my family for their encouragement and support throughout my academic endeavors.

REFERENCES

[1] M. Abid, and H. Afifi, "Secure E-passport protocol using elliptic curve Diffie-Hellman key agreement protocol," in *4th Int. Conf. on Inform. Assurance and Security ISIAS'08,* 2008, pp. 99-102.

[2] S.A. Anshuman, "A survey of system security in contactless electronic passports," *J. of Comput. Security, vol. 19*, no. 1, Feb. 2011, pp. 203-226. Available: http://iospress.metapress.com/content/8402gr10203t4236/. (Access Date: 4 May, 2012)

[3] A. Atanasiu, and M.I. Mihailescu, "Biometric passports (ePassports)," in *8th IEEE Int. Conf. on Commun. (COMM)*, Bucharest, Romania, 2010, pp. 443-446.

[4] V. Auletta et al., "Increasing privacy threats in the cyberspace: The case of Italian e-passports," in *Financial Cryptography and Data Security, vol. 6054*, Springer Berlin, Heidelberg, 2010, pp. 94-104.

[5] G. Avoine, K. Kalach, and J. Quisquater, "E-passport: securing international contacts with contactless chips," in *Financial Cryptography and Data Security, vol. 5143*, Springer Berlin, Heidelberg, 2008, pp. 141-155.

[6] C. Blundo et al., "Improved security notions and protocols for non-transferable identification," in *Computer Security ESORICS'08, vol. 5283*, Springer Berlin, Heidelberg, 2008, pp. 364-378.

[7] S. Boggan, (2008, August 06). Fakeproof e-passport is cloned in minutes. The Times. Available: http://www.thetimes.co.uk/tto/news/. (Access Date: 4 May, 2012)

[8] "Advanced security mechanisms for machine readable travel documents: EAC, PACE, and RI. v2.10," The German Federal Office of Information Security BSI, Tech. Guidelines, TR-03110-3, Mar. 2012.

[9] D. Carluccio et al., "E-passport: the global traceability or how to feel like a UPS package," in *Inform. Security Applicat., vol. 4298*, Springer Berlin, Heidelberg, 2007, pp. 391-404.

[10] J. Chapman, "Determining the security enhancement of biometrics in e-passports," in Bonn-Aachen Int. Center for Inform. Technology, Nov. 2009. Available: http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/09ws/09ws-sem/biometry-ws09-chapman.pdf. (Access Date: 4 May, 2012)

[11] T. Chothia, and V.A. Smirnov, "Traceability attack against e-passports," in *Financial Cryptography and Data Security, vol. 6052*, Springer Berlin, Heidelberg, 2010, pp. 20-34.

[12] J. Coron, et al., "Supplemental access control (PACE v2): security analysis of PACE integrated mapping," in *Cryptology eprint archive report 2011/058*, 2009. Available: http://eprint.iacr.org/2011/058.pdf. (Access Date: 4 May, 2012)

[13] "Israel cloned 1000s of UK passports and used airport security as mossad front," *European Union Times*, Mar 31, 2010, Available: http://www.eutimes.net/2010/03/israel-cloned-1000s-of-uk-passports-used-airport-security-as-mossad-front/. (Access Date: 4 May, 2012)

[14] G. M. Ezovski, and S.E. Watkins, "The electronic passport and the future of government-issued RFID-based identification," in *IEEE International Conference on RFID*, 2007, pp. 15-22.

[15] A. Fernandez-Mir, J. Castella-Roca, and A. Viejo, "Secure and scalable RFID authentication protocol," in *Data Privacy Manage. and Autonomous and Spontaneous Security, vol. 6514*, Springer Berlin, Heidelberg, 2011. pp. 231-243.

[16] L. Grunwald, "Security issues with RFID enabled passports and government issued eID documents, an overview of risk scenarios and attack vectors," *Neo Catena Networks Inc*., 2010. Available: https://media.blackhat.com/bh-ad-10/Grunwald/BlackHat-AD-2010-Grunwald-MRTD-eID-wp.pdf. (Access Date: 4 May, 2012)

[17] G.P. Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens," *J. of Computer Security (RFID Sec'10 Asia), vol. 19*, no. 2. 2011.

[18] V. Heino, "Moving to the third generation of electronic passports," *the Silicon Trust Gemalto*, 2011. Available: http://www.securitydocumentworld.com/client_files/moving_to_the_third_generation_of_electronic_passports_october_20111.pdf. (Access Date: 4 May, 2012)

[19] M. Hlavac, and T. Rosa, "A note on the relay attacks on E-passports: The case of Czech E-passports," *Cryptology eprint archive report 2007/244*, 2007. Available: http://eprint.iacr.org/2007/244.pdf. (Access Date: 4 May, 2012)

[20] M. Hlavac, "Known plaintext only attack on RSA–CRT with Montgomery multiplication," in *Cryptographic Hardware and Embedded Systems, vol. 5747*, Springer Berlin, Heidelberg, 2009, pp. 128-140.

[21] J. Hoepman et al., "Crossing borders: Security and privacy issues of the European e-Passport," in *Advances in Information and Computer Security, vol. 4266*, Springer Berlin, Heidelberg, 2006, pp. 152-167.

[22] M. Hutter, S. Mangard, and M. Feldhofer, "Power and EM attacks on passive 13.56 MHz RFID devices," in *Cryptographic Hardware and Embedded Systems, vol. 4727*, Springer Berlin, Heidelberg, 2007, pp. 320-333.

[23] "ISO/IEC 14443-4:2008 - Identification cards – Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol," *International Organization for Standardization*, 2008.

[24] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," in *IEEE Trans. on Circuits and Systems for Video Technology, vol.14*, no. 1, 2004, pp. 4-20.

[25] A. Juels, "RFID security and privacy: a research survey," *IEEE J. Selected Areas in Communications, vol. 24*, no. 2, 2006, pp. 381-394.

[26] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in E-passports," in *Proc. Anonymous Security and Privacy for Emerging Areas in Communications Networks*, 2005, pp. 74-88.

[27] P.A. Karger et al., "Security and privacy issues in machine readable travel documents," IBM Research Report, TR RC 23575 (W0504-003), , 2005. Available: http://domino.watson.ibm.com/library/CyberDig.nsf/papers/751B6341BFB9015485256FDB005DB216/$File/RC23575.pdf. (Access Date: 4 May, 2012)

[28] A. Laurie, "RF idiot", Available: http://rfidiot.org/. (Access Date: 4 May, 2012)

[29] D. Lekkas, and D. Gritzalis, "E-passports as a means towards the first world-wide public key infrastructure," in *Public Key Infrastructure, vol. 4582*, Springer Berlin, Heidelberg 2007, pp. 34-48.

[30] J. Leyden, "Code highlights E-passport eavesdropping risk: What RFIDIOt chipped my passport?," *The Register*, 2006. Available: http://www.theregister.co.uk/2006/10/31/rfid_e-passport_attack/. (Access Date: 4 May, 2012)

[31] J. Leyden, "RFID hack attack: E-passport cloning risks exposed,", *The Register*, 2006. Available: http://www.theregister.co.uk/2006/08/04/e-passport_hack_attack/. (Access Date: 4 May, 2012)

[32] I. Liersch, "Electronic passports – from secure specifications to secure implementations," in *Inform. Security Tech. Rep., vol.14*, no.2, 2009, pp. 96-100.

[33] Y. Liu et al., "E-passport: cracking basic access control keys," *On the Move to Meaningful Internet Systems, vol. 4804*, Springer Berlin, Heidelberg, 2007, pp. 1531-1547.

[34] L. Mirowski, J. Hartnett, and R, Williams, "An RFID attacker behavior taxonomy," *IEEE Pervasive Computing, vol.8*, no.4, 2009, pp. 79-84.

[35] P. Najera, F. Moyano, and J. Lopez, "Security mechanisms and access control infrastructure for E-passport and general purpose e-documents," *J. Universal Computer Science, vol.15*, no. 5, 2009, pp. 970-991.

[36] R. Nithyanand, "A Survey on the evolution of cryptographic protocols in ePassports," *Cryptology eprint archive 2009/200*, 2009. Available: http://eprint.iacr.org/2009/200.pdf. (Access Date: 4 May, 2012)

[37] V. Pasupathinathan, J. Pieprzyk, and H. Wang, "An on-line secure E-passport protocol," in *Information Security Practice and Experience, vol. 4991*, Springer Berlin / Heidelberg, 2008, pp. 14-28.

[38] I. Pooters, "Keep out of my passport: access control mechanisms in E-passports," 2008. Available: http://danishbiometrics.files.wordpress.com/2010/05/ivo.pdf. (Access Date: 4 May, 2012)

[39] "Protection profile for ePassport IC with active authentication," Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan,

2010. Available: http://www.commoncriteriaportal.org/files/ppfiles/c0247_epp.pdf. (Access Date: 4 May, 2012)

[40] H. Richter, W. Mostowski, and E. Poll, "Fingerprinting passports," 2008. Available: http://www.cs.ru.nl/~woj/papers/download/nluug2008.pdf. (Access Date: 4 May, 2012)

[41] H. Robroch, "ePassport privacy attack," Cards Asia Singapore, Apr. 2006. Available: http://www.riscure.com/archive/200604_CardsAsiaSing_ePassport_Privacy.pdf. (Access Date: 4 May, 2012)

[42] P.A. Rotter, "A framework for assessing RFID system security and privacy risks," *IEEE Pervasive Computing, vol.7*, no.2, 2008, pp. 70-77.

[43] B. Schneier, "How to clone and modify E-passports," Schneier on Security, Sep. 2008. Available: http://www.schneier.com/blog/archives/2008/09/how_to_clone_an.html. (Access Date: 4 May, 2012)

[44] B. Schneier, "RFID cards and Man-in-the-Middle Attacks," Schneier on Security, Apr. 2006. Available: http://www.schneier.com/blog/archives/2006/04/rfid_cards_and.html. (Access Date: 4 May, 2012)

[45] S. Sheetal, "Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues," 2006. Available: http://www-scf.usc.edu/~sheetals/publications/RFID_epassport.pdf. (Access Date: 4 May, 2012)

[46] The ICAO Secretary General, "Machine readable travel documents (MRTDs): History, Interoperability, and Implementation," ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-NTWG, 2007.

[47] The ICAO Secretary General, "Specifications for electronically Enabled MRTDs with biometric identification capability, Doc 9303, Machine Readable Travel Documents (MRTDs)," International Civil Aviation Organization, Part 3, Vol. 2, 2008.

[48] The ICAO Secretary General, "Supplement to Doc 9303, Machine Readable Travel Documents," ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-NTWG," Ver. 10, May 2011.

[49] The ICAO Secretary General, "Supplemental access control for machine readable travel documents – Technical Report, ISO/IEC JTC1 SC17 WG3/TF5 for ICAO, Ver. 1.01," November 2010.

[50] L. Thomson, "Hacker clones passports in drive-by RFID heist," V3 UK, Feb. 2009. Available: http://www.v3.co.uk/v3-uk/news/1953428/hacker-clones-passports-drive-rfid-heist. (Access Date: 4 May, 2012)

[51] M. Ullmann et al., "Password authenticated key agreement for contactless smart cards," Workshop on RFID Security, 2008. Available: http://events.iaik.tugraz.at/RFIDSec08/Papers/Publication/14%20-%20Ullmann%20-%20PW%20Authenticated%20Key%20Agreement%20-%20Paper.pdf. (Access Date: 4 May, 2012)

[52] P. Vijayakrishnan, J. Pieprzyk, and H. Wang, "Formal security analysis of Australian and E. U. E-passport implementation," in *Proc. 6th Australasian conf. on inform. security, vol. 81*, Australia, 2008, pp. 75-82.