Expert Systems with Applications 41 (2014) 5066–5070

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Cloning and tampering threats in e-Passports

Luca Calderoni *, Dario Maio

Department of Computer Science and Engineering, University of Bologna, Via Sacchi 3, 47521 Cesena, Italy

ARTICLE INFO

Keywords:
Safety/security in digital systems
e-Passports
Border controls
Electronic machine-readable travel documents

ABSTRACT

e-Passports present different security measures designed to safeguard their authenticity and more specifically to protect them from tampering and cloning attempts. Security protocols defined by *International Civil Aviation Organization* for this purpose (*Passive Authentication*, *Active Authentication*) should be enough to prevent such attacks. However, according to current specifications that regulate the *Logical Data Structure* of the e-Passport's chip, it is feasible to bypass these protocols exploiting some flaws in the *Inspection System*. In this paper we show that as long as new documents will not be issued in compliance with new logical data structure's specifications (currently under discussion), a careless implementation of the inspection procedure may lead to unsuccessful detection of cloned e-Passports.

1. Introduction

The specifications for e-Passport issuance were announced by *International Civil Aviation Organization* (ICAO) in 2004. ICAO is a specialized agency of the United Nations that sets standards and regulations necessary for aviation safety, security, efficiency and regularity, as well as for aviation environmental protection. Nowadays, more than 100 countries issue e-Passports and, according to ICAO, more than 500 million e-Passports are in circulation (International Civil Aviation Organization & 2013a. MRTD Report. Tech. Rep. 2, 2013a).

With the increase in the number of these documents the need arises to better understand their security and privacy implications. Border officers will need to handle electronic passports more and more frequently, which implies on one hand to provide them with instructions on how to perform border controls, and on the other hand to design expert and intelligent systems able to inspect and classify *electronic Machine-Readable Travel Documents* (eMRTD) properly. These systems are also referred to as *Inspection Systems* (IS).

From the outset, ICAO widely described security protocols designed to protect e-Passports from several kind of known attacks usually performed against electronic identity documents (International Civil Aviation Organization, 2006; International Civil Aviation Organization, 2008). Some of these attacks, such as *skimming*, *eavesdropping*, *data tampering*, *chip cloning* and *chip counterfeiting*, along with some of the related security and privacy issues, were discussed by Juels, Molnar, and Wagner (2005). From the border officers point of view, the most relevant security aspect is to be sure of the e-Passport authenticity, i.e. to be able to detect any attempt of chip counterfeiting, data tampering or chip cloning. These issues are addressed by two ICAO's protocols: *Passive Authentication* (PA) and *Active Authentication* (AA).

The design and implementation of e-Passport's chip and its content play a key-role in border security, and consequently in the design and implementation of the inspection system. Unfortunately, if the first issue is exhaustively addressed by several ICAO and BSI [1] official documents (International Civil Aviation Organization, 2006; International Civil Aviation Organization, 2008; Bundesamt, 2012), the second one is not. Official requirements for the design and implementation of the *Inspection System* are actually missing from literature (Frontex, 2011) and each country is supposed to implement his own following well-known best practices and some high-level procedures introduced in several technical reports (Liersch, 2009). This lack of clear guidelines can affect inspection systems interoperability and forms a threat to border security.

In the recent past, many feasible attacks against e-Passports were proposed. Most of them rely on some weakness in the *Basic Access Control* protocol (BAC), and mainly threaten the owner's privacy (Auletta et al., 2010; Chothia & Smirnov, 2010; Avoine, Kalach, & Quisquater, 2008; Liu, Kasper, Lemke-Rust, & Paar, 2007). As the security provided by BAC is limited by the design of the protocol itself, ICAO proposed a more secure access control protocol to be implemented in future released documents (International Civil Aviation Organization et al., 2010). A privacy threat was also

* Corresponding author.
E-mail address: luca.calderoni@unibo.it (L. Calderoni).

[1] Bundesamt für Sicherheit in der Informationstechnik, the German government agency in charge of managing computer and communication security for the German government.

http://dx.doi.org/10.1016/j.eswa.2014.02.044
0957-4174/

detected in relation to the *Active Authentication* protocol, as described by Monnerat, Vaudenay, and Vuagnoux (2007) and Bundesamt (2012).

In this paper we present a concrete form of attack that can be carried out exploiting some flaws in the inspection system, highlighting the consequences of the security flaw briefly discussed by International Civil Aviation Organization et al. (2011). More specifically, the attack relies on the cloning of the e-Passport's chip and a subsequent data tampering. As described in Section 3, if the *Passive Authentication* procedure implemented on the *Inspection System* does not perform a specific non-required check, the cloned passport could not be detected and no alert could arise on the system's display as well. Until each e-Passport in circulation will not comply the new *Logical Data Structure* (LDS) specifications, following the remarks published in International Civil Aviation Organization et al. (2011) about the removal of the file EF.COM from the LDS, each IS might be exposed to the attack proposed herein.

The aim of this paper is thus to provide some insight into the development and maintenance of inspection systems that are better suited to cope with the discussed attack.

2. Security protocols and logical data structure

The guidelines for e-Passport issuance are provided by the International Civil Aviation Organization (2006, 2008, 2013b), and include a detailed description of the security protocols and the LDS used to store and arrange data into the RFID (*Radio Frequency IDentification*) chip. This LDS stores information regarding the document's owner and the document itself, aside from some security information. The chip stores owner's personal data and biometric features, some optional information about the owner and the document and several elements used during the execution of the security protocols as the issuer's digital signature and its related certificate. Data are organized in several *Elementary Files* (EF), containing the information listed above; among these files, two are meta-files: the *Document Security Object* (SO_D), providing security information, and the plain, not signed, *Common Object* (COM), providing the LDS version and a list of the EFs stored in the chip, also referred as *Data Groups* (DG). These files are all contained in a *Dedicated File* (DF), called *e-Passport Application*, in its turn contained in the file system's *Master File* (MF) (International Organization for Standardization et al., 2013). In Fig. 1 we show a brief description of this data structure.

The security protocols handled by the chip are mainly designed to ensure its authenticity and integrity and to establish a secure communication channel between the RFID reader and the chip itself. These protocols rely on *Public Key Infrastructures* (PKI) and several cryptographic algorithms used to detect and prevent a wide range of malicious attacks. Each security protocol prevents a specific threat and exactly detects where, and in which way, the document has been attacked. Table 1 couples each protocol to the class of attack it prevents.

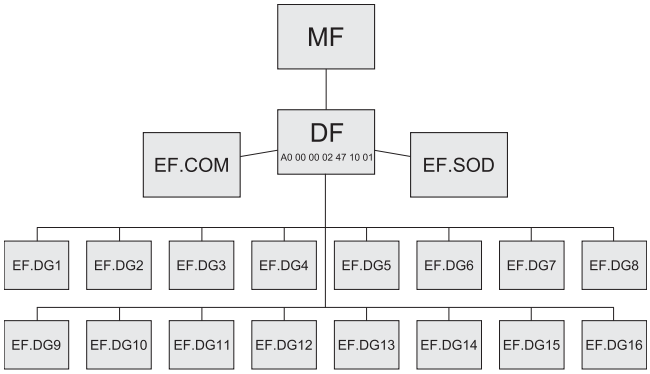

Fig. 1. The first version of LDS as described by ICAO.

For the purposes of this paper, it is appropriate to focus on the PA protocol and on the AA protocol.

2.1. Passive authentication

PA is designed to prevent and detect any attempt to tamper with the relevant data or to counterfeit the chip inside the document. This protocol relies on a trusted PKI widely described by Hartmann, Korting, and Katler (2009) and by Security Systems Division (2010), based on *X.509 Certificates* (Housley, Ford, Polk, & Solo, 1999, 2008). The authenticity and the integrity of the e-Passport's data are secured thanks to digital signatures. During the phase of chip customization, the hash of every DG present on the document is computed and stored inside the SO_D. Then these hashes are signed together using the private key of the *Document Signer* (DS); this signature is appended to the SO_D and can be verified thanks to the public key provided by the *Document Signer Certificate* (C_{DS}). C_{DS} is in turn signed using the private key of the *Country Signer Certification Authority* (CSCA). In order to validate its authenticity too, it is required to check its signature against the related public certificate (C_{CSCA}). The PA protocol can be summarized as follows:

(1) Read SO_D and derive C_{DS}.
(2) Verify that relevant data included in SO_D are intact checking SO_D signature against C_{DS}.
(3) Verify C_{DS} authenticity by checking its signature against C_{CSCA} (stored in the IS).
(4) Verify the validity of both C_{CSCA} and C_{DS} checking their expiry dates.
(5) For each relevant DG stored in the chip: calculate the fresh hash of the file content and check whether it matches the hash stored in the SO_D.

A more technical description of the protocol execution flaw is provided in Fig. 2. Due to the critical security aspects addressed by this protocol, ICAO states that PA is mandatory.

2.2. Active authentication

AA is designed to prevent chip cloning. In fact, it could be relatively trivial to read the chip content, extract all of the data and write them to a blank chip without corrupting the signatures of the SO_D. However, reading out of data is restricted to readable files shown in Fig. 1.

To implement this protocol it is required to generate an *Active Authentication Key Pair* (KPr_{AA}, KPu_{AA}). During the chip's customization phase, KPr_{AA} needs to be stored in the chip's secure memory while KPu_{AA} is stored in the *Data Group 15* (DG15). The

Table 1
e-Passports security protocols. Note that CA and TA are only available on European documents as they realize the EU *Extended Access Control* protocol.

Protocol	Abbrv.	Attack
Basic Access Control	BAC	Skimming
Secure Messaging	SM	Eavesdropping
Passive Authentication	PA	Chip Counterfeiting, Data Tampering
Active Authentication	AA	Chip Cloning
Chip Authentication	CA	Chip Cloning
Terminal Authentication	TA	Sensitive Data Theft