A Note on the Relay Attacks on e-passports*

The Case of Czech e-passports

Martin Hlaváč[1] and Tomáš Rosa[1,2]
hlavm1am@artax.karlin.mff.cuni.cz and trosa@ebanka.cz

[1] Department of Algebra, Charles University in Prague,
Sokolovská 83, 186 75 Prague 8, Czech Republic,
[2] eBanka, a.s., Na Příkopě 19, 117 19 Prague 1, Czech Republic

Abstract. The threat of relay attacks on authentication protocols is often well recognized, especially for contactless applications like RFID chips. It is, therefore, a bit surprising to meet an implementation that actually encourages rather than eliminates these attacks. We present our experimental observations concerning Czech e-passports. These show clearly an inherent weakness rooted in lower layers of ISO 14443. As the behavior is unavoidable, it induces a question on whether the e-passport should not have used a different communication protocol or authentication scheme.

Keywords : RFID, e-passport, relay attack

Introduction

Electronic passports based on a contactless proximity coupling smartcard technology (in short and a bit inaccurately called as RFID chips) according to ICAO standards [1] seem to be on an unstoppable rise. Long story short [2], these machine readable travel documents are equipped with an RF chip that stores a personal data of their owner. Access to this data shall be (at least in European Union countries) protected via a basic access control (BAC) mechanism to prevent their accidental skimming. The data are also digitally signed by an issuing authority to prevent their unauthorized change. This, of course, does not prevent copying these data into a "cloned" passport. Therefore, some countries decided to introduce so called active authentication (AA) protocol. Informally speaking, it is a challenge-response authentication based on RSA signature scheme with message recovery (ISO 9796-2). The RSA private key is protected by the chip, so it should be impossible to make a duplicate that passes AA verification.

Obviously, the scheme of AA can hardly avoid a relay attack as described e.g. in [3]. The approach described there actually behaves similarly to a plain wire-extender for a contact card. Using this technique, we can present an e-passport resting in somebody's pocket to a customs service without disturbing its holder

* The authors were supported by the grant from GAUK n. 7302/2007.

in any way. Therefore, the authentication scheme obviously does not assure the travel document authentication as was perhaps deemed by its architects. Unless we use distance bounding protocols [4], it is really hard to defeat these attacks. On the other hand, the distance for the attack seems to be limited physically as it is hard to imagine that it uses a TCP/IP or similar connection, since the relaying occurs on the link layer.

Our contribution is to show that it is not necessary to follow as general approach as in [3] to bypass the authentication protocol of a certain e-passport. We did this observation for Czech passports, but it is reasonable to expect that it will work for many other e-passports equipped with AA as well. First, it is easy to observe that all the data that needs to be relayed is the challenge and the response of AA. Everything else can be stored in the cloned chip locally. The core of the attack is that, due to a certain protocol behavior, there is much more time left for the resting transfers that what we would recognize in the general bit-by-bit approach. The short note elaboration presented here is an extension of the idea sketched in [5].

In section 1, the particular part of the ISO 14443 protocol used in the attack is described. Its concrete realization in chips of Czech e-passports is shown in section 2. One possible attack scenario is then given in 3. Finally, we conclude in 3.

1 Frame Waiting Time Extension

The transmission protocol between the terminal (the reader) and the RFID chip (the e-passport) is described in ISO 14443-4. After a successful initialization and anticollision procedure, the reader determines a communication attribute denoted `FWI` (Frame Waiting time Integer). The value of `FWI` is an integer in the range 0 to 14 (15 is RFU). For ISO 14443-A, it is obtained by sending `RATS` command (Request for Answer To Select) to the e-passport. When present, the interface byte `TB(1)` included in the e-passport's response `ATS` (Answer To Select) contains 4-bit value `FWI`. When `TB(1)` is not present, the default value 4 is used. For ISO 14443-B, the value of `FWI` is obtained during the anticollision procedure via `ATQB` response.

The `FWT` (Frame Waiting Time) is the *ordinary* maximum time period within which the passport has to start its responses to the terminal's commands during the protocol flow. It is defined as

$$\texttt{FWT} = (256 \times 16/f_c) \times 2^{\texttt{FWI}},$$

where $f_c = 13.56$ MHz is the carrier frequency. The allowable range for `FWI` yields the range for `FWT`, i.e. the minimal value is 302 μs and the maximal is 4.949 s.

As written in the standard: "*When the PICC needs more time than the defined `FWT` to process the received block it shall use an `S(WTX)` request for a waiting time extension.*" This request contains 6-bit value `WTXM` (Waiting Time eXtension

Multiplier) that yields a *temporary* value of FTW defined as

$$\texttt{FTW}_{\texttt{TEMP}} = \texttt{FTW} \times \texttt{WTXM}.$$

By the standard, the allowable values for WTXM are in the range 1 to 59. The reader has to acknowledge this temporary change by sending S(WTX) response containing the same value WTXM.

2 Czech e-passport and S(WTX)

When communicating with a Czech e-passport, it sets FWI = 10 within its ATS which yields FWT = 309 ms. After the BAC authentication is completed based on knowledge of (a part of) the machine readable zone (MRZ) of the passport, the active authentication protocol can start. The reader generates a random 8 byte challenge and sends it (encapsulated via a secure messaging) to the passport. Almost instantly ($< 36\mu s$), the passport sends back S(WTX) request with WTXM = 16, i.e. asking the reader to wait nearly 5 seconds for the answer. In order to be compliant with the standard, the reader has to accept this value.

In our experiments, the e-passport was usually able to start transmitting the AA response within 950 ms. When we provided it with limited field intensity, the response took less then 1250 ms (it probably saves energy by slowing down). One way or the other, there is roughly 4 s gap between the requested response period and actual response period opening the door to relay attacks. This issue is not an easy task to solve, as the readers have to be compatible with the existing e-passports.

3 Relay Attack Scenario

To exploit the unnecessary gap of 4 seconds in active authentication procedure, we can think of following scenario. A Czech visitor in a hotel in a foreign country leaves her passport at the hotel's reception. Having physical access to the passport (and its MRZ), the receptionist can access and copy all of the public data, i.e. namely the files DG1 (copy of machine readable zone), DG2 (biometric photography of the holder), DG15 (public key for AA) and EF.SOD (digital signature of the DG files by national authority).

Leaving the passport at the reception, one can cross the border identifying himself with the victim's passport in the following way. The attacker passes the BAC procedure simply by using the known MRZ data and provides the copy of DG files to the reader at the border. Consequently, he enters the AA protocol by receiving the AA challenge and relays it by a intermediate channel (e.g. TCP/IP) to a device at the reception which transmits it to the victim's passport. As the reader at the border has to be standard compliant and has to wait 5 seconds for the answer, there is enough time to relay the passport's answer back to it. We should also emphasize the possibility of using side band emulation technique to communicate with the passport reader [6]. That means that there does not have

to be any active chip in the document passed to customs. The communication can be established with a device held undisclosed in a handbag. Therefore, we can omit the demand that the cloned passport chip must fit into the cloned document itself. That, in turn, increases the chance of carrying out the whole attack in a practice considerably.

Note that the only two relayed messages are AA challenge and response, contrary to the approach described in [3]. All of the other commands can be done "off-line", i.e. without the communication with the victim's passport.

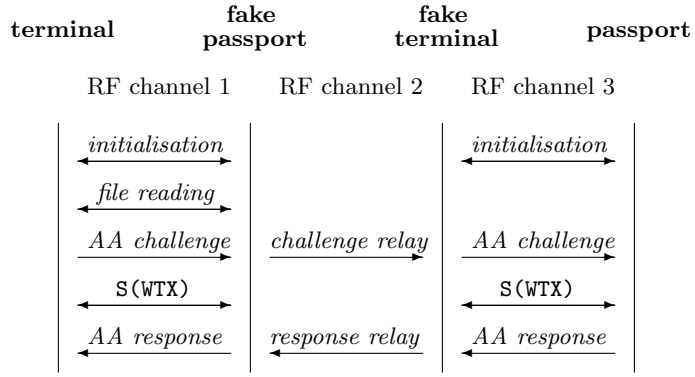

Fig. 1. Relay attack on active authentication (AA)

Conclusion

If we forget side channel techniques for a moment, then there is no known cryptanalytic method allowing a practically feasible attack on the active authentication scheme of e-passports. On the other hand, the general relay attacks clearly show that the proof of private key possession does not imply a proof of the travel document originality. We showed that particular communication protocol properties can even make these attack considerably more dangerous. The question arises whether a protocol like ISO 14443 that was obviously designed with very little or no security concerns is the right choice for such applications. A tighter union of the protocol itself and the used cryptographic schemes would be perhaps desirable.

References

1. International Civil Aviation Organization. http://www.icao.int/.
2. Gildas A. Security and Privacy in RFID Systems. http://lasecwww.epfl.ch/ gavoine/rfid/, 2007.

3. Hancke G. A Practical Relay Attack on ISO 14443 Proximity Cards. http://www.cl.cam.ac.uk/ gh275/relay.pdf, 2007.
4. Brands S. and Chaum D. Distance-bounding protocols. In *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 344–359, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.
5. Klíma V. and Rosa T. Elektronický cestovní pas: autentizace. *Sdělovací Technika*, (5), 2007.
6. Kfir Z. and Wool A. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems. Cryptology ePrint Archive, Report 2005/052, 2005. http://eprint.iacr.org/.