E-passport: Security attacks

[State of art]

Aquiles Ricardo TORRES ALVAREZ[*]
Grenoble INP - ENSIMAG
Grenoble, Francia
torresaa@

Jorge Luis GULFO MONSALVE[†]
Grenoble INP - ENSIMAG
Grenoble Francia
gulfomoj@

ABSTRACT

General Terms

Theory

Keywords

passport, MRT, RFID, ICAO, eavesdropping, BAC, attack, cryptography

1. INTRODUCTION

2. TECHNICAL BACKGROUND

2.1 RFID

The way the E-passport works is by communicating with a RF reader which emits a wave that feeds the contactless chip (as mentioned at [8], because is the only one that meets the ICAO's requirements) located at passport which is a Radio Frequency ID (because it is meant to be unique) or tag. Once he is feeded the exchange of information begins but without protection of any other around RF reader's eavesdropping, that means someone that could scan that information. So, knowing all possibles security issues and privacy threats attached to the data exchanged between the e-passport and the reader, the **ICAO** (*International Civil Aviation Organization*) , which is the organization that sets all the protocols and standards for the e-passport, has established a set of protocols such as *Passive Authentication* (PA), *Basic Access Control* (BAC), *Active Authentication* (AA) and *Extended Access Control* (EAC) for encrypting the information exchanged between the RFID chip and the reader keeping the privacy and security of the e-passport holder.

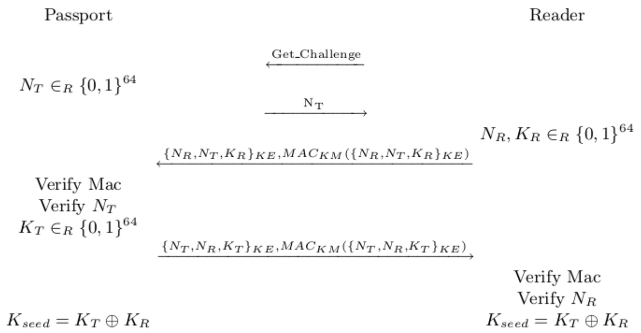
Passport
Reader
Get_Challenge
$N_T \in_R \{0,1\}^{64}$
$\mathrm{N_T}$
$N_R, K_R \in_R \{0,1\}^{64}$
$\{N_R, N_T, K_R\}_{KE}, MAC_{KM}(\{N_R, N_T, K_R\}_{KE})$
Verify Mac
Verify N_T
$K_T \in_R \{0,1\}^{64}$
$\{N_T, N_R, K_T\}_{KE}, MAC_{KM}(\{N_T, N_R, K_T\}_{KE})$
Verify Mac
Verify N_R
$K_{seed} = K_T \oplus K_R$
$K_{seed} = K_T \oplus K_R$

Figure 1: BAC protocol sesion.

As mentioned at [8] the first protocol to treat was *PA*, which signs the passport with a public key of the issuing country in order to prove the integrity and authenticity of the data.

2.2 BAC Protocol

As mentioned at [1], *BAC* which is a protocol that prevents skimming by encrypting the data with two symmetric keys (K-ENC and K-MAC) that are derived from the passport's *MRZ* (Machine Readable Zone) (birthdate, the passport's expiry date and the alphanumeric passport number). Once the reader is authenticated all the passport information of the holder are contemplated.

As we can see at the figure 1 once the tag receives the challenge from the reader, he answers by some encrypting information with the keys KE and KM where the reader has to be able to prove the knowledge of the keys from the MRZ. When the tag proves the authenticity, a session key KS-Seed is generated to encrypt all the communication.

2.3 Ative Authentication

As mentioned at [6], in order to prevent cloning the *AA* protocol was created. This protocol is more an anti-cloning feature because here the passport must prove to the reader that he has a private key as a response to a challenge previously received.

2.4 Extended Access Control

In [8] is mentioned that in next generation e-passports EAC has being used instead of BAC because before proceeding with the same steps as BAC he verifies the authenticity of

[*] Electrical student at Universidad del Norte - Colombia. Double major student of Telecommunication at Ensimag - France

[†] Electrical student at Universidad del Norte - Colombia. Double major student of Telecommunication at Ensimag - France

the reader by a certificate validation from the issuing passport's country, certificate which must be transmitted in a safe way.

3. E-PASSPORTS ATTACKS

3.1 Cryptographic Weaknesses

As we know, the *Basic Access Control (BAC)* protocol establishes a secured channel between the *RFID* tag and the reader in order to provide confidentiality and integrity to the data communication. *BAC protocol* generates the encryption and authentication keys from the data present in passport's *MRZ* (number, expiration, date of birth) and it is demonstrable that the entropy of this data don't reach at least the 80 bits suggested and can be worse with simple observations [6] [7].
Liu, Kasper and others [7] had made a complexity analysis of the key space focused on demonstrate the low entropy of *BAC keys* for two main passport's nationality: Germany, Netherlands but easily extensible to other countries. The low entropy of key is caused first by the use of mainly numeric characters on passport number, second because of the stochastic dependency between passport number and its expiration date, and finally due to dependency of publicly available personal data. The analysis showed that in the best case, we know only public information and issuing state, the entropy reach **52.8 bits** for the German's passports but it can fall to **20.4 bits** for Netherlands passports if we have a *BAC keys database*. This low entropy is more disturbing when they estimated the time to find the *MRZ* in 25h and less than 185ms respectively.

3.2 Traceability

One of the most serious problem of e-passport is the possibility to trace them, that means that attackers are able to identify a passport that they knew before. According to Chothina and Smirnov [2] this is possible because of the wireless lecture system of these *MRTD (Machine Readable Travel Document)*.

The most interesting argument of these authors [2] is that we can identify the passport using the security system that it uses to avoid unauthorized readers: *BAC*. The attacker only need to record (eavesdropping) a session between the passport and an authorized reader (one that has access to MRZ), it can be done from a distance of 25m [7], and when they come across another passport they send the ***GET CHALLENGE*** *message* in order to get a nonce that the attacker will answer with the recorded message. As the *ICAO standard* specifies that passports have to answer to all message using **ISO 7816** error codes, such as *"6A80: Incorrect parameters"* or *"6300: No information given"*, them the answer of passport to recorded message will be useful to identify him because they send a specific message when *MAC check* fails or rises (french passports) or maybe because the answer time is greater when *MAC check* succeed. In both cases, if *MAC check* is correct we are addressing to the same passport.

All this attacks have been made without any victim's passport contact, and the closest communication (BAC challenge) is possible a 50cm away [2].

3.3 Physical-layer Weaknesses

All the information that we can extrait from e-passport is a potential threat for the owner or for the national security of the country (expediter or receptionist) but this information is not necessary linked to cryptographic process in *MRTD*, sometimes it is more accessible than we think. This is the case of the attacks to communications protocols in physical layer, maybe useful with all *RFID tags* but when they are linked to e-passports they can give us additional information.

First we can talk about Danev, Heydt-Benjalin and Capkun [4] work, they have tested their method to identify the manufacturer of RFID smart cards with an equal error rate of 2.43%. This error rate makes the RFID transponders identification possible in practical situations including e-passports. The attacker only need a recorded signal and then the statistic analysis of spectral features. There are not a lot of RFID manufacturers and, of course, nations have to buy the RFID tag of their e-passports to some of them. If we can determine the manufacturer of the smart card in the passport then we will be closer to identify its nationality. This information will be useful to determine the MRZ as we have seen before 3.2.

In the other hand, in logical level the communication reader-passport use *Applications Protocol Data Units (APDUs)* which are specified in *ISO 7816* standard. Of course this standard have some status words defined like *"No error (9000)", "Unknown(6F00)"* and more but the *ICAO* guidelines for e-passports are not specific about the logical response to every command, that is the reason why all nations have the freedom to use the *APDUs* as they want. This liberty to chose the response of logical commands makes possible to Richter, Mostowski and Poll [9] identify the nationality of passport using a set of 7 commands and watching the answer of every passport to them. Ten passports's nationlities have been identified by using this little command set; in order to increase the number of known nationalities would be necessary to use some others commands which is still possible.

3.4 Cloning

As mentioned in [5], once the reader and the tag have passed BAC, AA is implemented. As it was already mentioned the objective of this protocol is to the prevent cloning, so once the reader sends the challenge to the tag it responds immediately responds with a WAIT message leaving a gap of five seconds which finally are about four seconds because the tag takes approximately one second to perform the private key validation. So a possible scenario (as dictated at [5]) is when somebody for example at an hotel forgets his passport at the reception, somebody at the reception could have access to the MRZ sends those values to somebody at the border and with a device registers that, passes the BAC and once at AA he replays all messages from the reader to and from the true passport all of that in even in less than four seconds.

4. CONCLUSIONS

HELLLO DFDFDFDFDF [3]

5. REFERENCES

[1] D. Carluccio, K. Lemke-Rust, C. Paar, and A.-R. Sadeghi. E-passport: The global traceability or how to

feel like a ups package. In J. Lee, O. Yi, and M. Yung, editors, *Information Security Applications*, volume 4298 of *Lecture Notes in Computer Science*, pages 391–404. Springer Berlin Heidelberg, 2007.

[2] T. Chothia and V. Smirnov. A traceability attack against e-passports. In *Proceedings of the 14th International Conference on Financial Cryptography and Data Security*, FC'10, pages 20–34, Berlin, Heidelberg, 2010. Springer-Verlag.

[3] T. Chothia and V. Smirnov. A traceability attack against e-passports. In R. Sion, editor, *Financial Cryptography and Data Security*, volume 6052 of *Lecture Notes in Computer Science*, pages 20–34. Springer Berlin Heidelberg, 2010.

[4] B. Danev, T. S. Heydt-Benjamin, and S. Čapkun. Physical-layer identification of rfid devices. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, pages 199–214, Berkeley, CA, USA, 2009. USENIX Association.

[5] M. Hlavac and T. Rosa. A note on the relay attacks on e-passports: The case of czech e-passports. In *IACR Eprint archive*, 2007. hlavm1am@artax.karlin.mff.cuni.cz 13688 received 19 Jun 2007, last revised 24 Jun 2007.

[6] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, SECURECOMM '05, pages 74–88, Washington, DC, USA, 2005. IEEE Computer Society.

[7] Y. Liu, T. Kasper, K. Lemke-rust, and C. Paar. E-passport: Cracking basic access control keys with copacobana.

[8] N. Maria. Rfid chips and eu e-passports: the end of privacy? 2012.

[9] H. Richter, W. Mostowski, and E. Poll. Fingerprinting passports.