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

2.2 BAC Protocol

2.3 Ative Authentication

2.4 Extended Access Control

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 provided 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 [4] [5].

Liu, Kasper and others [5] 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 at the of the study they estimate 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 of trace them, that means that attackers are able to identify a passport that they know before. According to Chothina and Smirnov [1] this is possible because of the wireless lecture system of these *MRTD (Machine Readable Travel Document).*

The most interesting argument of these authors [1] 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 [5], and when they come across another passport they send the ***GET CHALLENGE** message* in order to get a nonce that attacker will answer with the recorded message. Als the *ICAO standard* specify 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 an specific message when *MAC check* fail or rise (french passports) or maybe because the answer time is greater is *MAC check* succeed. In both cases, if *MAC check* is correct we are addressing to the same passport.

All this attack has been made without any victim's passport contact, and the closest communication (BAC challenge) is possible a 50cm away [1].

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

[*] 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

layer, maybe useful with all *RFID tags* but when are linked to e-passport the can give us additional information.

First we can talk about Danev, Heydt-Benjalin and Capkun [3] 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 specify 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 because 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 [6] 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

4. CONCLUSIONS

HELLLO DFDFDFDFDF [2]

5. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

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