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 [2] [3].

Liu, Kasper and others [3] 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

3.3 Physical-layer Weaknesses

3.4 Cloning

4. CONCLUSIONS

HELLLO DFDFDFDFDF [1]

5. REFERENCES

[1] 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.

[2] 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.

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

*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