Security of Biometric Passports

Team Members :
Aniruddha Harish
Divya Chinthalapuri
Premdeep Varada

Introduction and Motivation:

A biometric passport combines paper and electronic storage, wherein the biometric information of a person is stored on an electronic chip(usually an RFID), which is then used to authenticate the identity of travellers. The use of Biometric Passports is becoming the base for secure authentication of personal identity. It uses contactless smart card technology, which includes a microprocessor chip and antenna on the passport. Countries are required to build a Public Key Infrastructure, biometric and Radio Frequency Identification which is used to authenticate the data stored electronically in the passport chip and hence making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented.

Since 2006, there have been development of 3 generations of electronic passports and the distribution of over 30,000,000 electronic passports. Though many standards are included by the ICAO and security measures are implemented from time to time; there are shortfalls in the current e-passports issued by various nations. As E-passports contain important private information and are directly related to nation's security and border control; protection of data is extremely essential. Therefore, we analyze the cryptographic protocol sets in each of these generations and explore the ways to enhance the privacy and security of this technology.

List of E-passport implementations we are planning to explore:

Implementations of three generations of biometric passports and compare each generation
How the Dutch electronic passport has been attacked by a Dutch firm.

Detailed description of problems/hypotheses we are planning to investigate:

Research on the cryptographic protocols implemented in each of the three generations of E-passports.
Research on finding effective ways to enhance the privacy and security of biometric passports.

Hypothesis to be investigated:

The possible attacks in a biometric passport can happen during the communication between the RFID chip on the passport and the reader placed at the airport authority.

1. ISO standardized the distance between the e-passport and the reader to be 10 cm. Since the RFIDs are passive devices, hostile attackers can design unauthorized readers capable of skimming the contents from a greater distance.

2. Traceability attack is possible which exploits an e-passport that allows attackers remotely to track a given credential in real time without first knowing the cryptographic keys that protect it.
3. Cloning of the e-passport is possible by substituting the chip of an e-passport with a fake chip storing the data copied from the chip of another e-passport.

All the above attacks are studied in detail by considering different hypotheses situations.

Tentative list of questions we will be seeking answers to:

What is Biometric passport and how is it used to control border security?
How is it more secure compared to the currently used paper based passport?
What is the necessary public key infrastructure for the use of biometric passports.
What are the security threats and attacks that the biometric passports are vulnerable to?
How is this technology enhancing its standards of security to ensure privacy and prevent fraud in each generation?

- Passive Authentication
- Active Authentication
- Basic Access Control
- Extended access control
- Data encryption

What are the e-passport cryptographic protocols in use and what needs to be enhanced for better protection? This is analysed by comparing how the biometric passports of few nations have been attacked.

Procedure for verifying the results of our investigation:

Going through the literature all that is available and by comparing results obtained from implementations, previously verified case studies, research papers, and scholarly papers.
Relying on opinions of the experts.

Time schedule, including intermediate goals to be achieved by the dates of progress reports:

Oct. 15-17:

Investigating previous research and comparing all the cryptographic protocols used for each generation for this technology.
Analyzing each attack in detail : cause and effect; in order to figure out the areas of threat.

Nov. 5-7

With the material acquired till date, after our analysis, we would come up with the feasible solution for better protection of biometric passports; in terms of detailed presentation of proposed solutions and cryptographic protocols.
Creation of a draft of the report.

Nov. 19-21:
Future scope and upgrade
Creation of finalized report and presentation slides by Nov 21

A list of possible areas, where the specification can change depending on the progress of the project:

- First Generation & Second generation E-passport Security Vulnerabilities
- We might come up with more than one solution while working on different attacks.

Tentative table of contents of your final report:

1. Introduction
2. What is a biometric passport?
3. Implementation of biometric passports for border control.
4. PKI of biometric passports.
5. Cryptographic protocols used in different generations of passports.
6. Security threats and attacks.
7. Effective ways to enhance the privacy and security.
8. Role of biometric passports in the future.
9. Conclusion
10. References

List of literature:

[1] Md.Monzur Morshed, Anthony Atkins, Hongnian Yu, " Privacy and Security Protection of RFID Data in E-passport*", in Software, Knowledge Information, Industrial Management and Applications (SKIMA), 2011 5th International Conference on 8th-11th September.*
[2] (2012) in Review. Biometric ID Systems Grew Internationally, And So Did Concerns About Privacy.[Online]Available:https://www.eff.org/deeplinks/2012/12/biometric-id-systems-grew-internationally-2012-and-so-did-concerns-about-privacy4
[3] S. Kc. Gaurav and Paul A. Karger," Security and privacy issues in machine readable travel documents (MRTDs)," *IBM T. J. Watson Research Labs, IBM Technical Report (RC 23575), April 2005.*
[4] György Kálmán, Josef Noll ," On Privacy Protection in Biometric Passports" *in 2009 Third International Conference on Digital Society.*
[5]V.K Narendira Kumar, B.Srinivasan,"Security Mechanisms and Access Control Infrastructure for Biometric Passport using Cryptographic Protocols" *in 2013MECS conf Available:(http://www.mecs-press.org).*
[6] Md.Monzur Morshed, Anthony Atkins, Hongnian Yu, " Privacy and Security Protection of RFID Data in E-passport", *in Software, Knowledge Information, Industrial Management and Applications (SKIMA), 2011 5th International Conference on 8th-11th September.*
http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=6089991

[7] G. Matthew Ezovski and Steve E. Watkins, " The Electronic Passport and the Future of Government-Issued RFID Based Identification", *at the 2007 IEEE International Conference on RFIDinTexas,USA.*Available:http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=4143505