

ePassport security under the microscope

Matthew Sirotich

Introduction

- ▶ What is RFID, where is it being used and why?
- ▶ Security implications of RFID
- ▶ Why is it being used to secure passports?
- ▶ The methodology used to assess ePassports and create its successor
- ▶ ePassports security breaches
- ▶ The proposed ePassport
- ▶ The Irony of it all
- ▶ Concluding statements

What is RFID, where is it being used and why?

- ▶ A Radio Frequency Identification Tag (RFID) is a “tiny, inexpensive chip that transmits a uniquely identifying number over a short distance to a reading device, and thereby permits rapid, automated tracking of objects” (Jules, 2005 p. 1)

What is RFID, where is it being used and why?

- ▶ RFID has multiple applications through multiple sectors:
- ▶ Defence:
 - logistics, inventory control, asset management and tracking of vehicles (Administration, 2005).
 - RFID is also being assessed for human centric applications (Christensen, 2006).

What is RFID, where is it being used and why?

▶ Business

- RFID has been coined the predecessor of the optical barcode (Jules, 2006 p. 381) and hence has vast implementations in the Business to Business and Business to Consumer industry
- Logistics, inventory control etc.

▶ Consumer sector

- Innovations providing efficiency such as the RFID library.
- More radically, some have implanted themselves to automate daily authentication regimes such as logging into their computer (Graafstra, 2007).

What is RFID, where is it being used and why?

- ▶ It is being used in all these sectors because the technology facilitates non line of sight identification.

Security implications of RFID

- ▶ Researchers such as Jules (2005), Lamb (2006), Thornton (2006), Molnar (2005) and Karjoth (2005) are already describing the inherent weaknesses of RFID technology

Security implications of RFID

- ▶ The major threats posed by RFID systems are:
- ▶ Tracking
 - the act of following a tags movements based upon its UID response to interrogations
- ▶ Inventorying
 - allowing a user to identify object(s) being carried by another person.

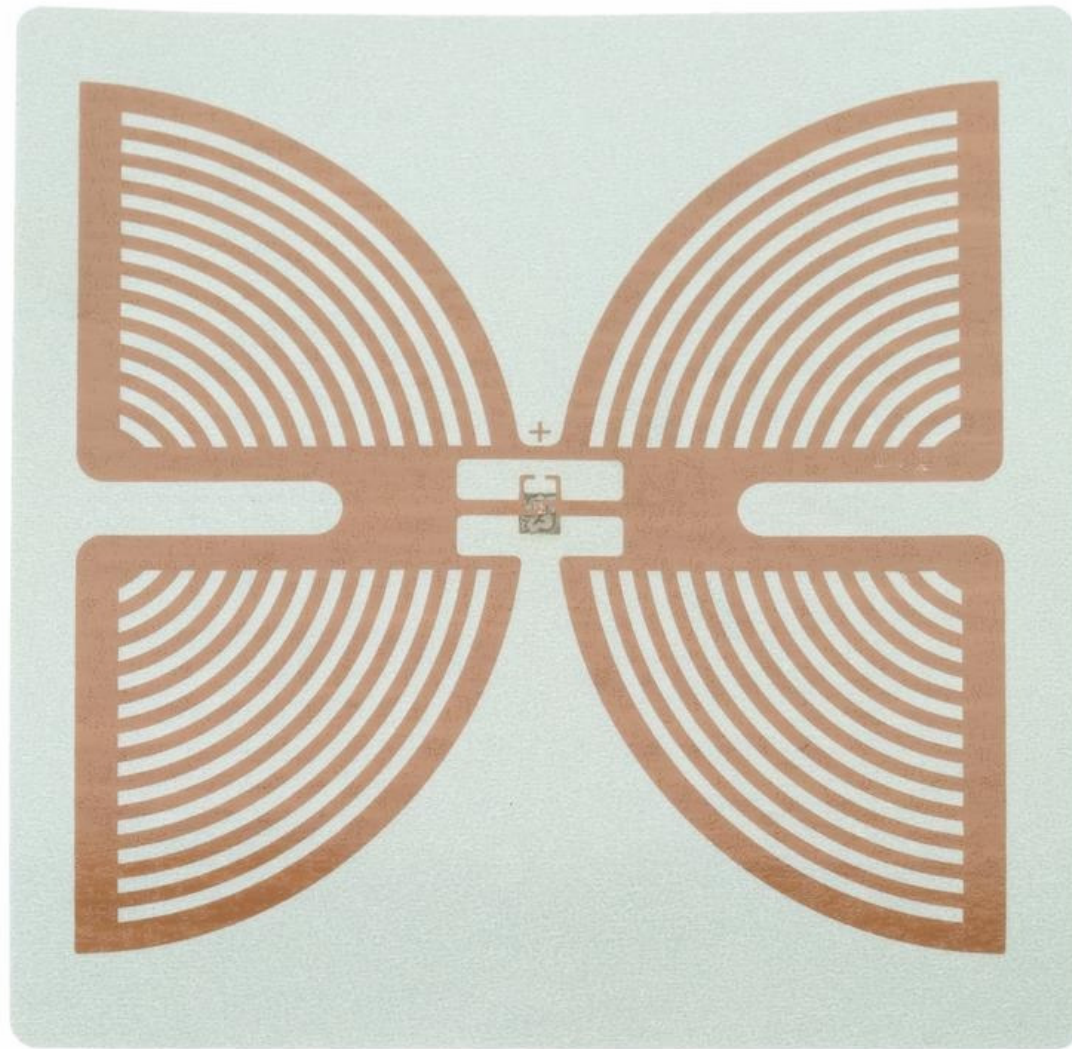
(Jules, 2005).

Why is it being used to secure passports?

- ▶ The rationale behind RFID in passports as documented by the Australian Government's department of foreign affairs is:
 - To provide protection against tampering and misuses
 - Reduce identity fraud
 - Enhance border protection
 - Provide a fast and efficient passport verification system

Why is it being used to secure passports?

	New Passport	Old Passport
Misuses	Provides added security to stamp out misuses	Occurs frequently
Identity Fraud	Reduces the occurrence	Occurs frequently
Border Protection	Provides more cumbersome protection due to enhanced passport	Provides protection, but has been known to let the wrong people in
Speedy verification	A lot faster (even self service)	Slow process in comparison



The methodology used to assess the ePassport and create its successor

- ▶ To use quantitative experimentation to prove the insecurities of current ePassport technology.
- ▶ Qualitative representations of this data will then be used to perform a security audit of current ePassport technology. The findings, along with the qualitative data were used to influence the construction of the proof of concept.
- ▶ The proposed solution was finally compared to the current ePassport to determine which best provided privacy and security to its users.

ePassports security breaches

- ▶ Firstly, it is important to assess the underlying technology.

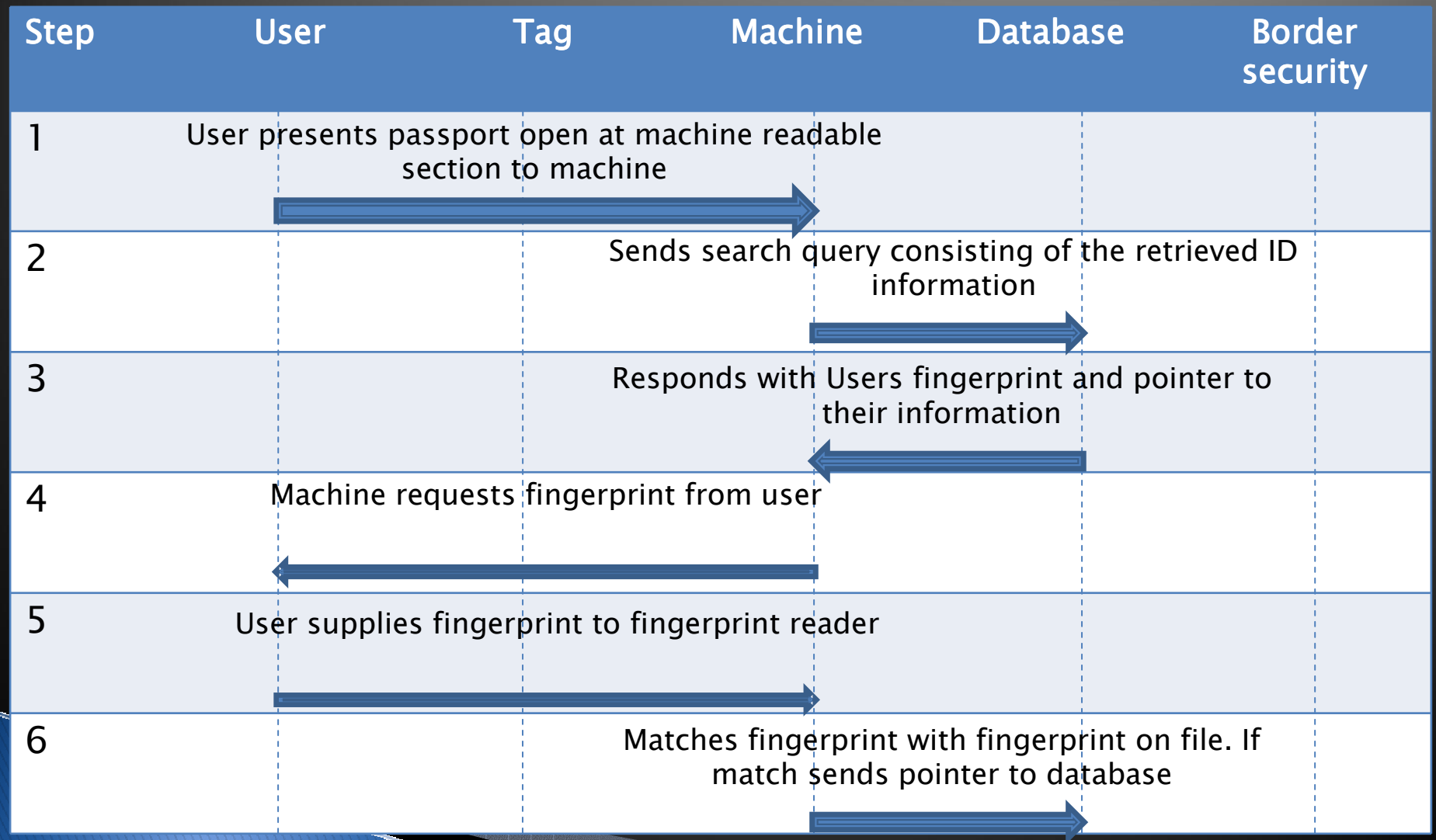
Experiment	Measurement
Injection attack	Breach
Blocking a reader	Breach
Skimming a tag	Breach
Killing a tag	Breach
Flooding a reader	Resisted Breach
Copy and mimic a tag	Breach

ePassports security breaches

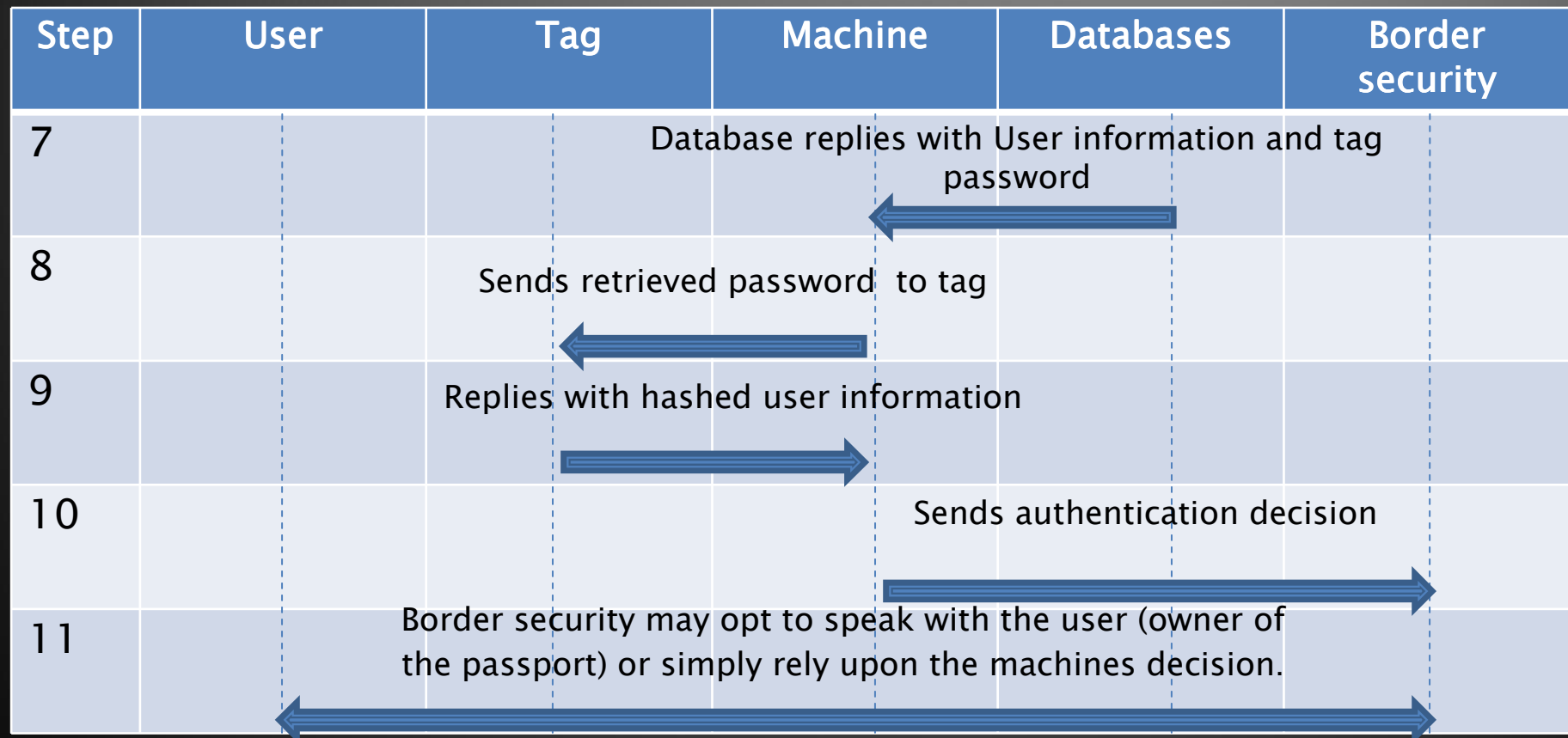
- ▶ It is now possible to apply this information to the ePassport to define security breaches and to assess the impact of these breaches.

Security Breach	Does it impede on the privacy and security meant to be provided by the ePassport?
Skimming	A user could be followed and profiled, a smart bomb could be created if commonalities in data were found.
Injection attack	A database could be destroyed hence rendering the ePassport system useless.
Faraday cage failing	The failing Faraday cage in the current ePassport allows for rogue reading in stealth.
Killing a tag	A tag can be killed and hence reduce an ePassport back into a paper-based passport. Hence no added security.
Copying a tag and mimicking	An ePassport could be copied and the encryption taken home to be used in an offline attack to decrypt the data.

The proposed ePassport



The proposed ePassport



The proposed ePassport

- ▶ Questioning ePassport's key
 - 3DES military standard encryption
 - ICAO decided that the key was to comprise of a concatenation of the passport number, holders date of birth, and passport expiry date (in that particular order).

The proposed ePassport

- ▶ The proposed implementation uses message digests that can never give away the original text.
- ▶ Then isn't it possible to copy someone's message digest and use it as your own? Yes, but:
 1. Have to know the unique password for the ePassport he/she was trying to copy; and
 2. Have to have the same fingerprint as the legitimate user; and
 3. Have to look exactly like the legitimate user.

The proposed ePassport

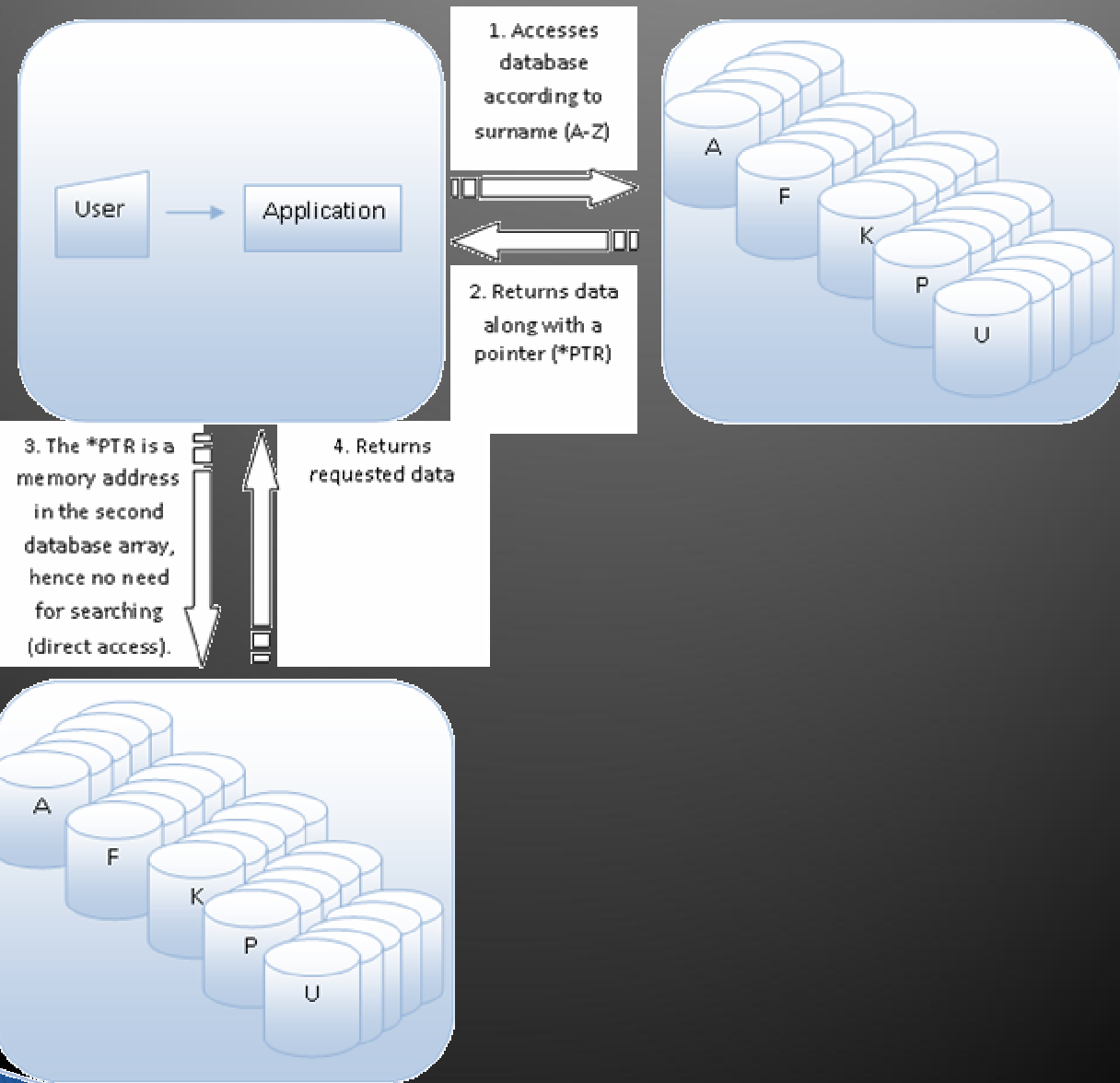
- ▶ Security provided by the system:
 - Layer 1 – Unique user query in the database
 - Layer 2 – Biometric test, a searchprint is taken and compared to the fileprint
 - Layer 3 – Tag verifies itself by responding to the correct password that is sent randomly
 - Layer 4 – Data preservation via message digest

The proposed ePassport

- ▶ Privacy preservation layers:
 - Layer 1 – Password protected tag prevents rogue reads
 - Layer 2 – Data is message digested and hence can never be used to gain information
- ▶ Integrity provided
 - Multi stage authentication verification process, compares stored data to retrieved data
- ▶ Availability provided:
 - Only a bona-fide user can access the tag due to the password protection.
- ▶ Policy prevents use of damaged RFID tag

The proposed ePassport

► Databases



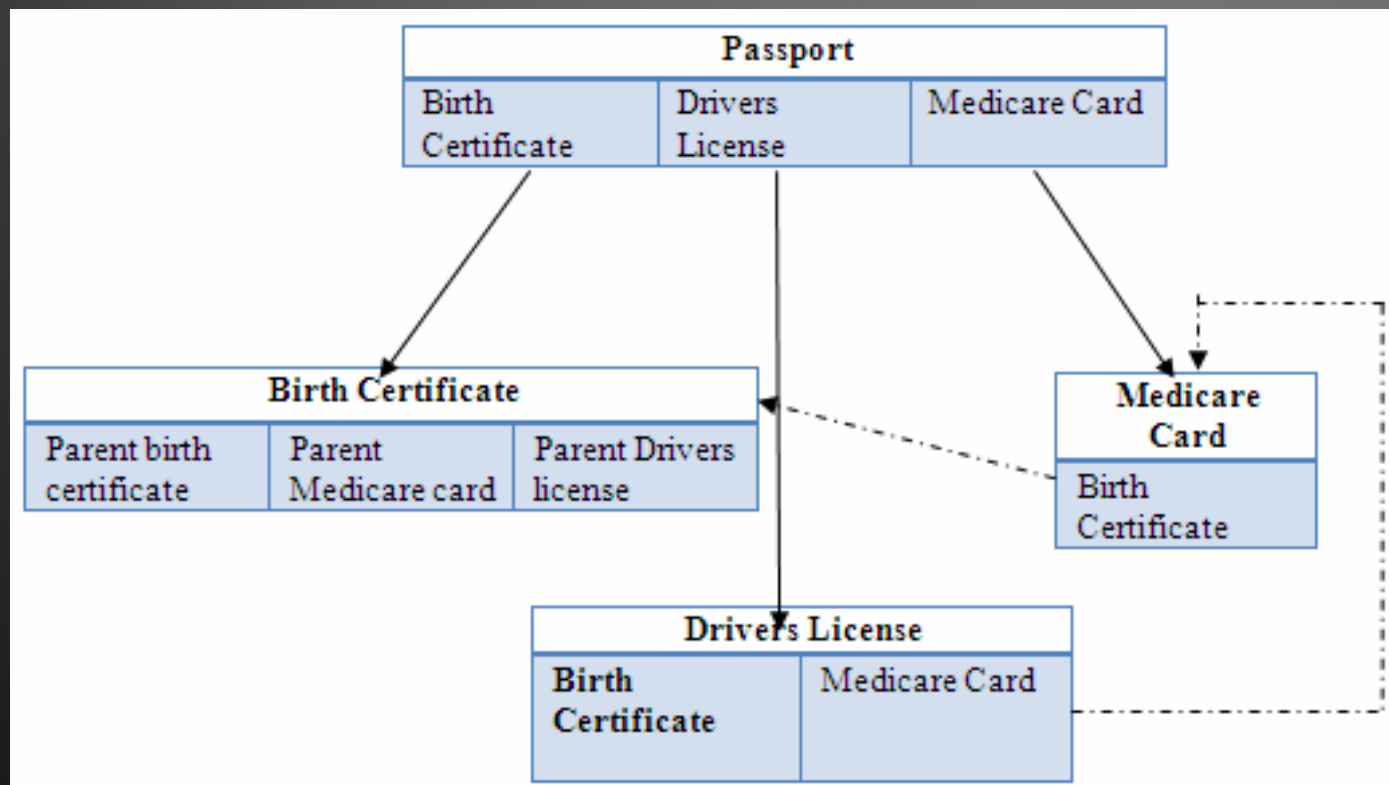
The proposed ePassport

- ▶ Comparison of current ePassport to proposed ePassport

Possible security breach	Current ePassport	Proposed ePassport
Tracking	Breach	Resisted Breach
Killing	Breach	Resisted Breach
Injection attack	Breach	Breach
Blocking security device	Breach	Resisted Breach
Wave injection attack	Breach	Breach
Steal information	Breach	Resisted Breach
Flooding	Resisted Breach	Resisted Breach
TOTAL	Breach=6, Resisted Breach=1	Breach=2, Resisted Breach=5

The irony of it all

- ▶ Seminal documents must be revised.



Concluding statements

- ▶ ePassport's are currently insecure and reduce the privacy and security of the user
- ▶ The proposed ePassport addresses the found security breaches and should be implemented
- ▶ The reliance each seminal identification document has on each other and the chronological progression of their gathering needs review.

References

- ▶ Jules, A. 2005. *RFID Privacy: A technical primer for the non-technical reader*. MA : RSA Laboratories, 2005.
- ▶ Christensen, B. 2006b. VeriMed Implanted RFID Dogtags Studied By Military, VeriChip. *Technovelgy*. [Online] 2006b. [Cited: 4 12, 2007.] <http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=722>.
- ▶ Administration, Federal Highway. 2005. Technologies Supporting Military Deployments. *FHWA office of operations*. [Online] 2005. [Cited: 4 12, 2007.] http://ops.fhwa.dot.gov/opssecurity/dev-mx/chapter_5.htm.
- ▶ (Graafstra, A. 2007. Hands on: How Radio-Frequency Identification and I got personal. *IEEE Spectrum*. 2007, pp. 15–19.
- ▶ Lamb, G, M. 2006. New 'e-passports' raise security issues ; Despite official assurances, some worry that thieves might read chip- toting US passports. Boston : s.n., 2006, p. 13.
- ▶ "RFID Security. Thornton, F. Haines, B. Das, A, M. Bhargava, H. Campbell, A. Kleinschmidt, J. 2006. Rockland : Syngress Publishing Inc, 2006.
- ▶ Molnar, D. Soppera, A. Wagner, D. 2005. Privacy for RFID through Trusted computing. *Workshop on Privacy in the Electronic Society*. November 7, 2005.
- ▶ Karjoth, G. Moskowitz, A, P. 2005. Disabling RFID Tags with Visible Confirmation: Clipped tags are silenced. *Workshop on Privacy in the Electronic Society*. November 7, 2005.