Physical-layer Identification of RFID Devices

Boris Danev
bdanev@inf.ethz.ch

Thomas Heydt-Benjamin
hey@zurich.ibm.com

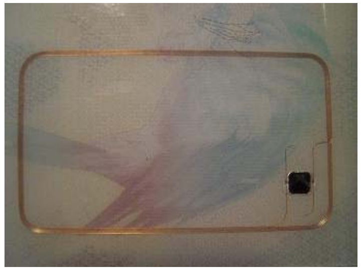
Srdjan Capkun
capkuns@inf.ethz.ch

Agenda

1. ePassport Overview
2. ePassport Security
3. Problem Statement
4. RFID Fingerprinting
5. Experimental Evaluation
6. Application to ePassports
7. Conclusion

1. ePassport Overview

- The ePassport
  - Contains a purpose-built RFID chip
  - That stores personal information (e.g., name, date of birth) and biometrics (e.g., fingerprint, face scan)
  - The content is accessible via a standardized wireless interface (ISO 14443 Type A and Type B)
- The International Civil and Aviation Organization (ICAO) standardizes the content
  - EF.DG1: personal information (required)
  - EF.DG2: picture (required)
  - EF.DG[3-14,16]: fingerprints, iris scans (optional)
  - EF.COM: index of available files



2. ePassport Security (1/2)

- Passive Authentication (ICAO required)
  - **Data integrity**
  - Stores hashes of the information and a public key, hashes are digitally signed with a private key
- Basic Access Control (ICAO optional)
  - **Data confidentiality**
  - Key = Document number + Date of birth + Date of expiry
  - Messages are encrypted using 3DES and contain MACs
- Active Authentication (ICAO optional)
  - **Cloning prevention**
  - RSA public and private key pair. The private key is stored in the inaccessible chip memory
  - Challenge-response protocol

2. ePassport Security (2/2)

- Cloning ePassports without Active Authentication
  - Lukas Grunwald, *BlackHat 2006*
  - Bit by bit copy of content in a self-written ePassport emulator
  - Can be prevented by using Active Authentication
- Retrieving secret ePassport data
  - Marc Witteman, *What the Hack 2008*
  - Using power analysis to retrieve the private key
- Read ePassports with predictable document numbers
  - Adam Laurie reads BAC protected UK passport
  - An educated guess (sequential document numbers)
- ePassports Reloaded
  - J. Van Beek, *BlackHat Asia 2008*
  - Attacks on the Passive and Active Authentication

3. Problem Statement

- The Questions
  - Can we identify (fingerprint) a RFID chip at the physical layer?
  - What identification accuracy can be expected?

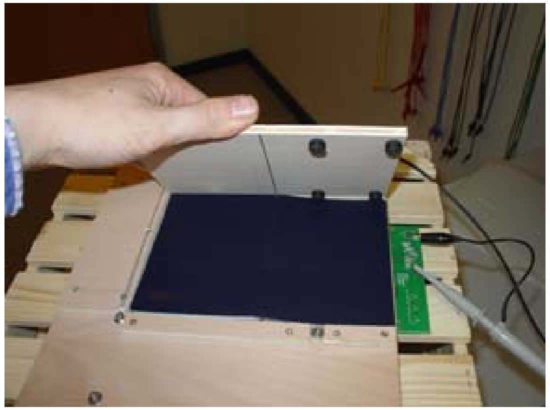
- Motivations
  - Information can be easily copied, but hardware is more difficult
  - From human biometrics to hardware “biometrics”

- Current status
  - Hardware setup for signal acquisition
  - Implementation of a fingerprinting RFID tag reader
  - Feature extraction and matching algorithms

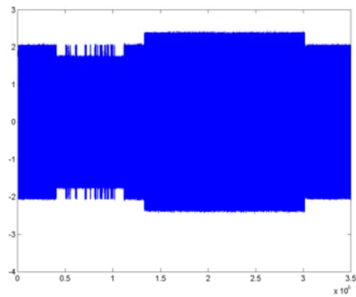
4. RFID Fingerprinting (1/3)

- Signal Acquisition Setup

Purpose-built HF (13.56MHz)
RFID Reader
ISO 14433 Type A and Type B



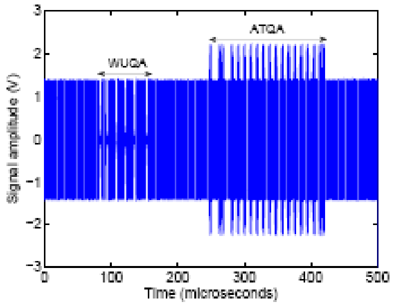
Acquisition antenna setup



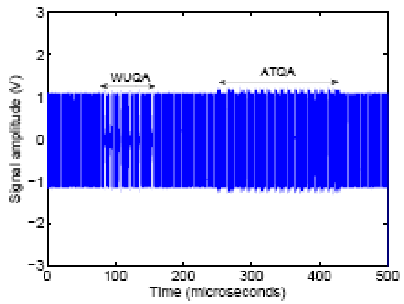
Captured signal transmission

4. RFID Fingerprinting (2/3)

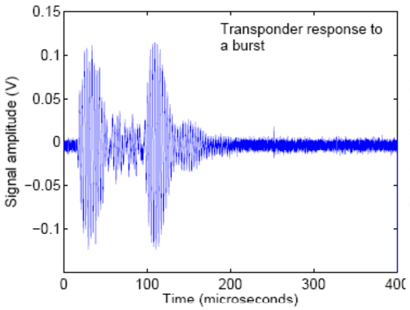
- Experiments performed
  - Experiment 1 (Standard)
    - Fc = 13.56 MHz
  - Experiment 2 (Varied Fc)
    - Fc = 12.86 – 14.36 MHz
  - Experiment 3 (Burst)
    - Sinusoidal burst of RF energy
  - Experiment 4 (Sweep)
    - Sinusoidal frequency sweep of RF energy



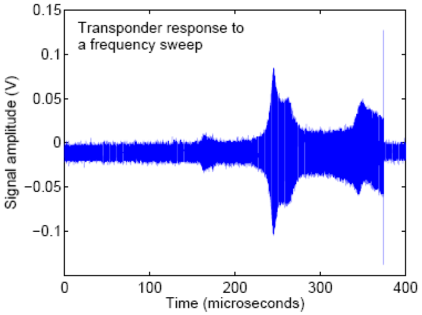
Standard



Varied Fc



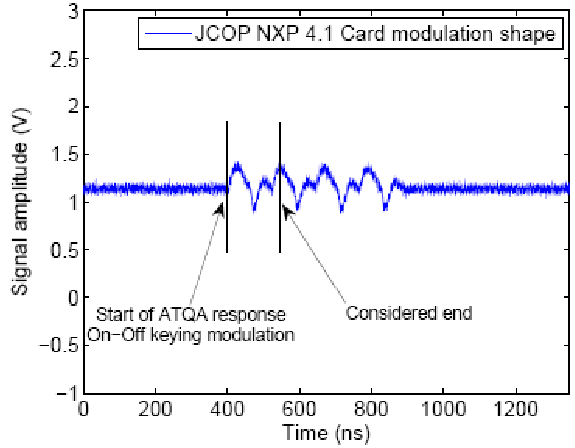
Burst



Sweep

4. RFID Fingerprinting (3/3)

- Timing Features
  - Measuring time between reader query and chip response
  - At different carrier frequency (Fc = 12.86 – 14.36 MHz)
- Modulation-shape Features
  - Type A response is On-Off keying
  - Extract the shape of the On-Off keying by Hilbert transformation



- Spectral Features
  - Extract frequency information
  - Burst and sweep frequencies are selected by means of Fourier transformation and high-dimensional Principal Component Analysis

5. Experimental Evaluation

- Data Sets

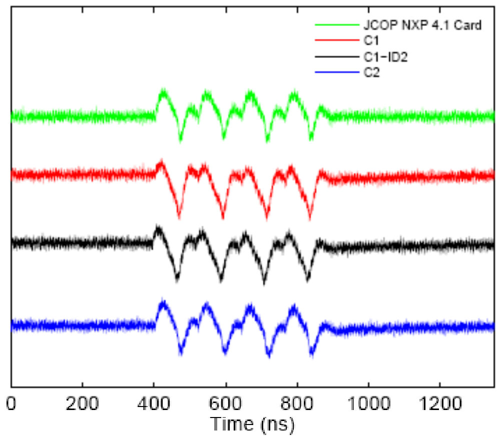
Table 1: RFID device populations (passports and JCOP NXP smart cards).

Type	Number	Label	Country	Year	Place of Issue
Passport	2	ID1, ID2	C1	2006	P1
	1	ID3	C1	2006	P2
	1	ID4	C1	2006	P3
	1	ID5	C1	2007	P4
	1	ID6	C2	2008	P5
	1	ID7	C3	2008	P6
	1	ID8	C1	2008	P1
JCOP	50	J1..J50	JCOP NXP 4.1 cards (same model and manufacturer)		

- Evaluating Accuracy
  - Classification (e.g., country of issuance, year, etc)
  - Identification (i.e., identify individual passports)

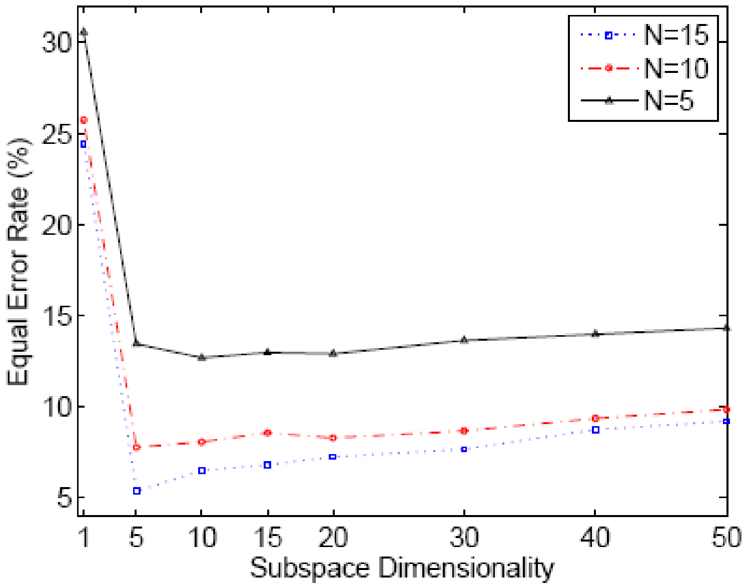
5.1. Classification Accuracy

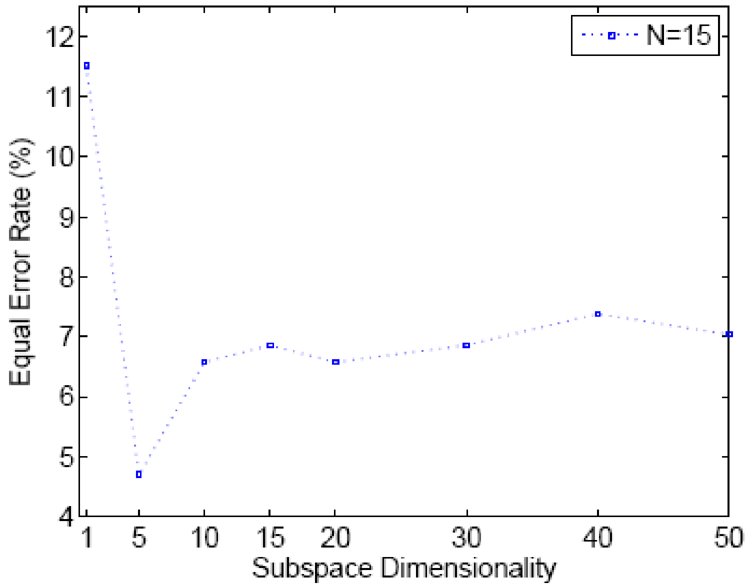
- 4 different classes
  - 8 ePassports from **3** countries + 10 JCOP cards = **4** classes
- Classification accuracy
  - Timing features
    - Very low classification accuracy
    - Each country seems to use RFID chips from same manufacturer. The standard is well implemented
  - Modulation features
    - High classification accuracy (100%)
    - Different RFID chips?
    - However even passports within same country exhibit
    - differences in the modulation



5.2. Identification Accuracy (1/2)

- 50 JCOP NXP 41 cards
  - Same model and manufacturer
- Burst and Sweep features
  - Equal Error Rate (EER) = 5% (i.e., 95% accurate identification)



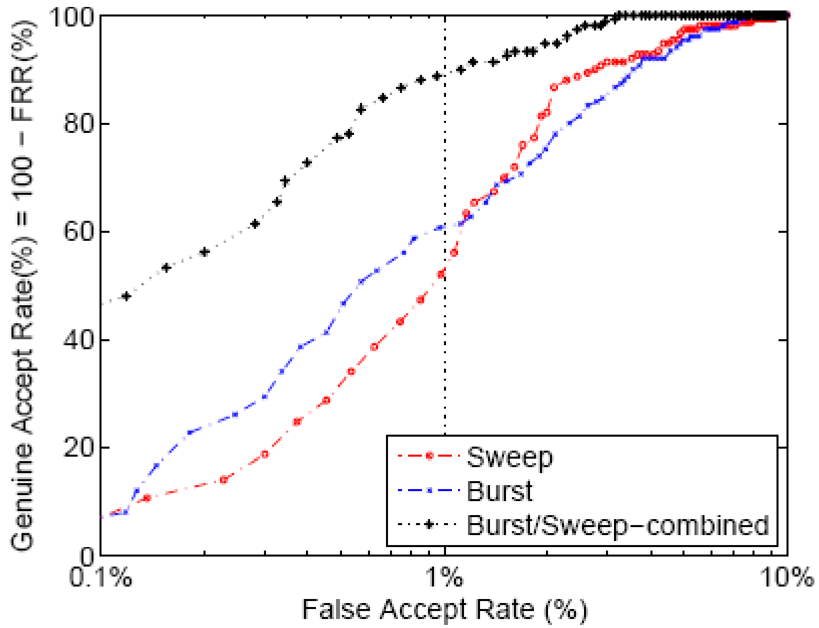


5.2. Identification Accuracy (2/2)

- Combining Burst and Sweep Features
  - **EER** improves to **2.4%**
- Receiver Operating Characteristic (ROC)
  - Shows the improvement for various False Accept Rates(FAR) and False Reject Rates (FRR)

FAR	FRR	GAR = 100%- FRR
0.1%	50%	50%
1%	10%	90%
>5%	0%	100%

Table 1: Recognition Accuracy



6. Application to ePassports

- ePassport cloning detection
  - **Scenario 1:** The RFID fingerprint is stored in back-end database
    - Measured before deployment
    - Stored in back-end database, indexed by the ID of the transponder
    - Online verification
  - **Scenario 2:** The RFID fingerprint is stored on the transponder.
    - RFID fingerprint size = 120 bytes.
    - Stored in the chip memory (36/72KB EEPROM in NXP chips)
    - The fingerprint integrity should be ensured, i.e. digitally signed by the document-issuing authority
    - Offline verification

7. Conclusion and Future Work

- Passive RFID transponders exhibit unique features on the physical layer due to manufacturing variability.
- Such variations are inherent even to identical (same model and manufacturer) transponders.
- Future work needs to address a number of issues:
  - Can we improve the identification accuracy?
  - How hard is to reproduce an RFID physical-layer fingerprint? (e.g., radio signal replaying)
  - Additional attacks and countermeasures

- Q & A