



E-Passport: The Global Traceability or How to Feel Like an UPS Package

Dario Carluccio, Kerstin Lemke-Rust,
Christof Paar, and Ahmad-Reza Sadeghi

Horst-Görtz Institute for IT Security

July, 14th 2006

Workshop on RFID Security



Current Situation

- Security and privacy problems have been pointed out by experts
- Successful attacks have been mounted on
 - e.g., on Netherlands e-passport by Riscure
- Most security mechanisms are optional
- Trust Model and relations have changed
 - new parties involved such as service providers, CAs
- No complete security analysis including trust relations available publicly
- Future plans require update of chip data (visa information) but not analyzed thoroughly and publicly

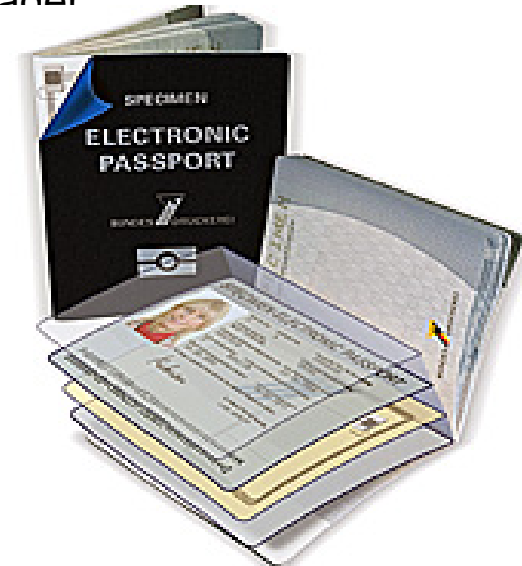
Our goal

- **Revisit privacy problems (Germany as use case)**
- **Present feasible devices to exploit vulnerabilities of current implementation of Basic Access Control**
 - **enables large scale tracing of e-passport holders**
- **To draw public and authorities' attention to existing problems and to care when employing a new technology for citizens in security critical areas**



Overview of E-Passport

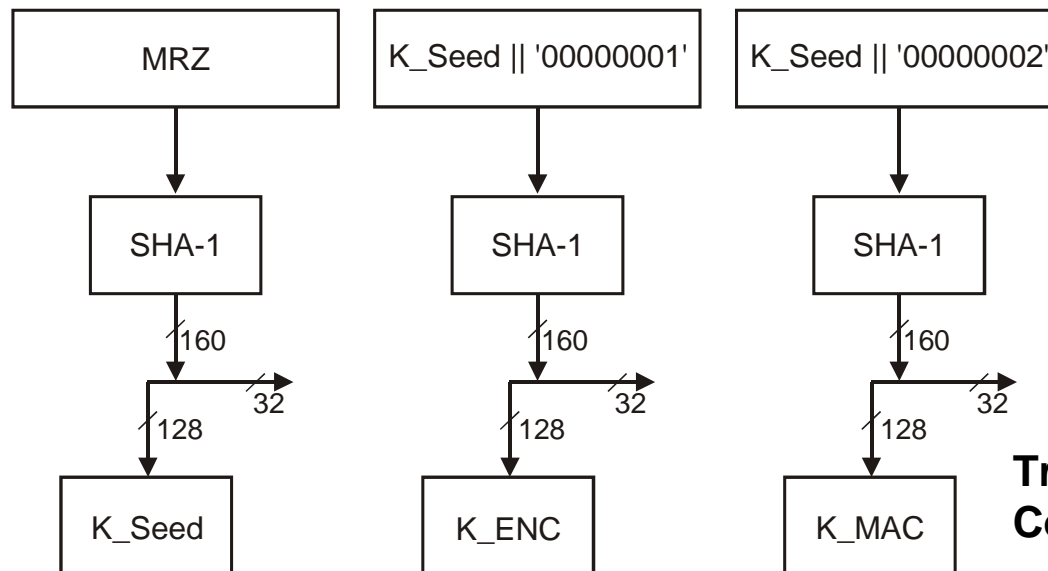
- RFID Communication between secure chip and reader
- Distance passport – reader < 30cm
- Stored data on chip
 - Name
 - Passport No
 - Date of birth
 - Date of expiry
 - Biometrical data (facial Image, fingerprint, ...)
- Main cryptographic components
 - Passive Authentication (mandatory)
uses digital signature by issuer (data signed)
 - Active Authentication (optional)
deployed against anti-cloning
 - Basic Access Control (BAC) (optional)
establish secure RFID communication
 - Extended Access Control (ratified recently)
chip and terminal authentication





Basic Access Control (BAC)

- Prevent unauthorized read access
- Key derived from data printed on the passport
(note: only a **part** of Machine Readable Zone MRZ)
 - Passport No
 - Date of birth
 - Date of expiry
- Only an optional feature (specification)



Triple DES Keys for Basic Access Control



BAC: Protocol Overview

Reader (IFD)

MRTD (ICC)

RND_{ICC}

$RND_{ICC} \in_R \{0,1\}^{64}$

$RND_{IFD} \in_R \{0,1\}^{64}, K_{IFD} \in_R \{0,1\}^{128}$

$S_{IFD} := RND_{IFD} \parallel RND_{ICC} \parallel K_{IFD}$

$E_{IFD} := E_{K_{ENC}}(S_{IFD})$

$M_{IFD} := MAC_{K_{MAC}}(S_{IFD})$

$A := E_{IFD} \parallel M_{IFD}$

Decrypt and Verify $E_{IFD} \parallel M_{IFD}$

$K_{ICC} \in_R \{0,1\}^{128}$

$S_{ICC} := RND_{ICC} \parallel RND_{IFD} \parallel K_{ICC}$

$E_{ICC} := E_{K_{ENC}}(S_{ICC})$

$M_{ICC} := MAC_{K_{MAC}}(S_{ICC})$

$B := E_{ICC} \parallel M_{ICC}$

$KS_{Seed} := K_{IFD} \oplus K_{ICC}$

Decrypt and Verify $E_{ICC} \parallel M_{ICC}$

$KS_{Seed} := K_{IFD} \oplus K_{ICC}$



Key Entropy

- Part of MRZ used for BAC (Germany):

x1x2x3x4 **y1y2y3y4y5** p<< **jjmmtt** p<< **jjmmtt** p<<

- **x1x2x3x4** Behördenkennzahl BKZ (local agency number)
- **y1y2y3y4y5** Serial number of passport
- **jjmmtt** Date-of-birth
- **jjmmtt** Date-of-expiry (10 years)

- Entropy model for BAC

- Date of Expiry depends on Serial Number of each BKZ
- However, for BKZ assumptions should be made
⇒ Reducing entropy
- Further entropy reduction possible
 - Age can be guessed
 - City of residence can be guessed (at airport)

www.pruefziffernberechnung.de

- Use cases for this work

- Netherlands: 35 bit entropy
- Germany: 40 bit - 51bit entropy (conservative estimation)
- Further breakdowns possible depending on assumptions



Tracking System

- Threat
 - Ability to trace individuals by eavesdropping, recording and breaking the Basic Access control
 - Collecting information stored on chip in a database accessible over Internet
- Who is interested in tracking and such databases
 - Criminal organizations and terrorists
 - Detectives
 - Commercial data mining agencies
- Technical requirements
 - Eavesdropper device
 - Can record communication between reader and e-passport from several meters
 - Installation at places with high e-passport density (e.g., at airports) may need collaborators, e.g., insiders, maintenance and cleaning personal
 - MRTD Cracker
 - Performs key searching remotely



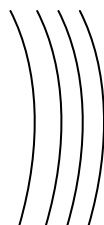
Basic Idea of Tracking System



**RFID
eavesdropper**

Database

MRTD Cracker



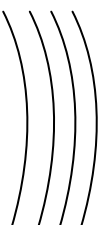
**Date, Time,
Location,
encrypted
MRTD Data**



**encrypted
MRTD Data**



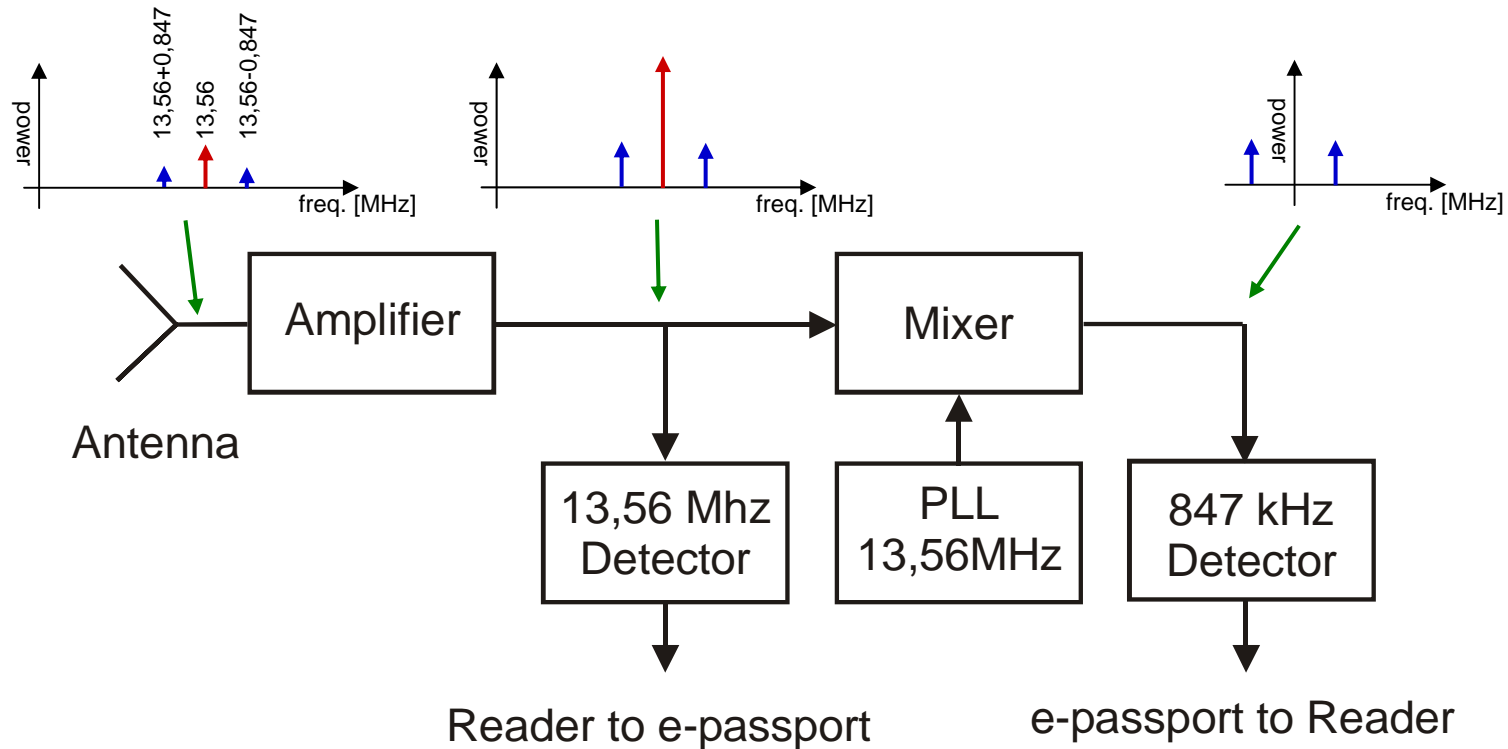
**Plain MRTD Data
(name, date-of-birth, facial image)
and Encryption key**



**Eavesdropping
communication
(basic access control)**



RFID Eavesdropper



PLL = Phase Locked Loop (used as 13,65 MHz signal generator)

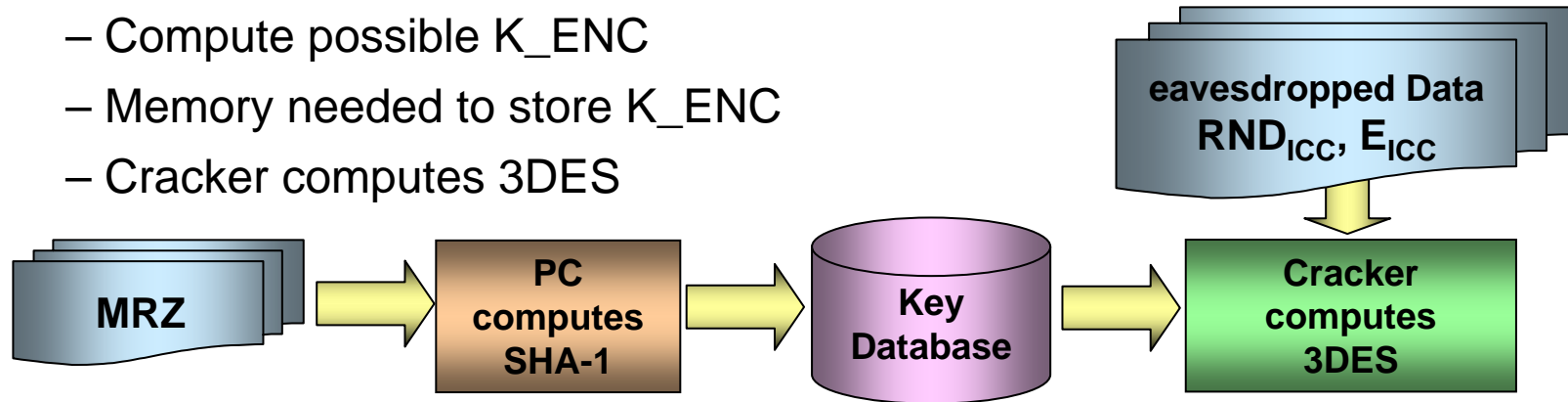
Range of eavesdropper: a few meters depart from inspection system



MRTD Cracker

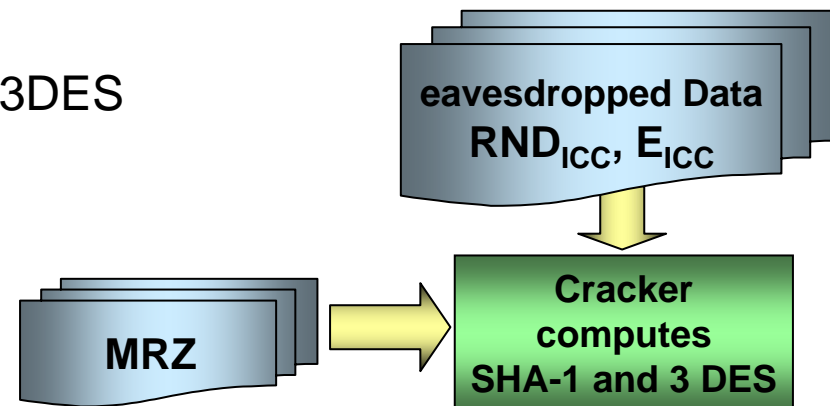
- **With precomputation**

- Compute possible K_{ENC}
- Memory needed to store K_{ENC}
- Cracker computes 3DES



- **Without precomputation**

- Cracker computes SHA-1 and 3DES





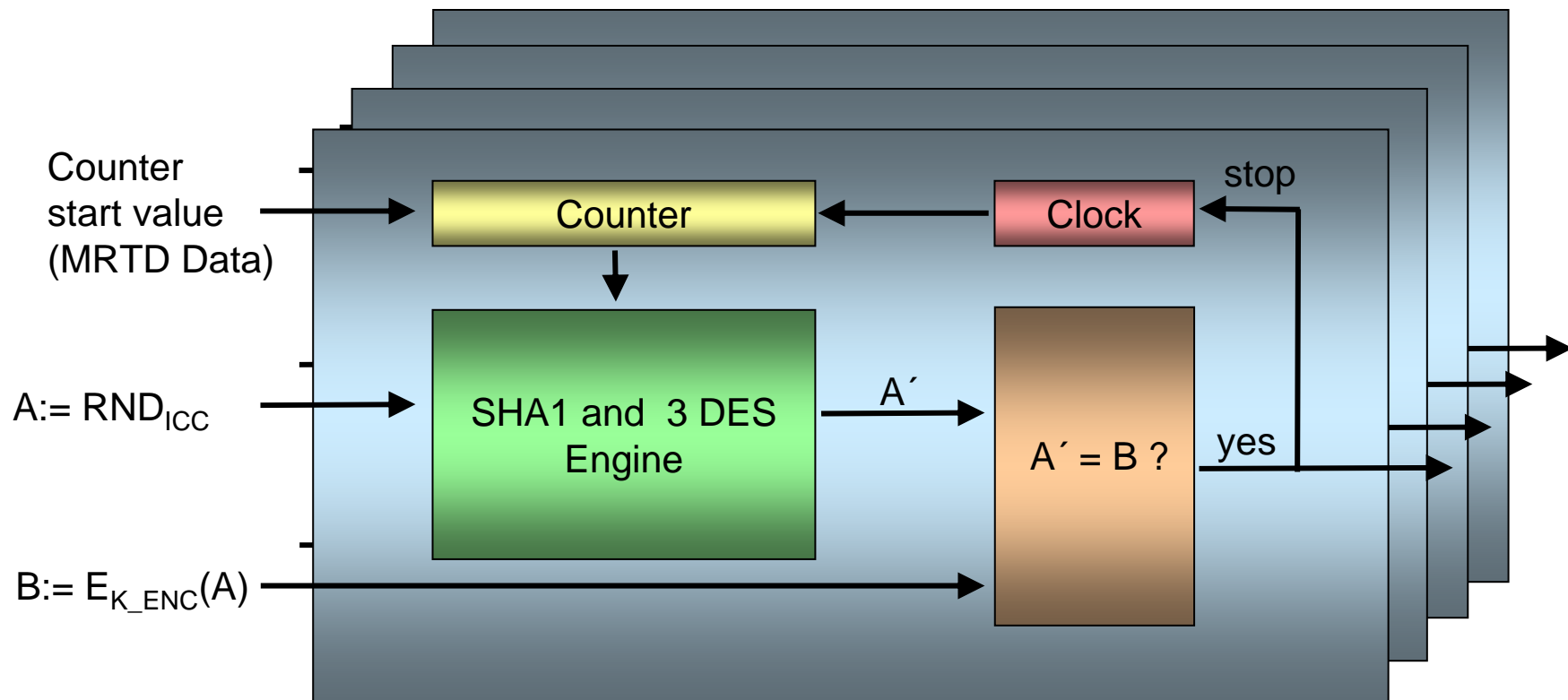
Implementations of Cracker

- **Software based**
 - Low engineering cost
 - Distributed computing
(computing nodes must be trusted)
- **Hardware based**
 - ASIC
 - cheap for large scale
 - high non recovering engineering costs
 - FPGA
 - flexible architecture
 - reasonable costs
 - adaptation of Cost Optimized Parallel Code Breaker (COPACOBANA)



Hardware based mrtd craker

- Specialized cost efficient Hardware to compute $E_{ICC} := E_{K_ENC}(RND_{ICC})$ without pre-computation



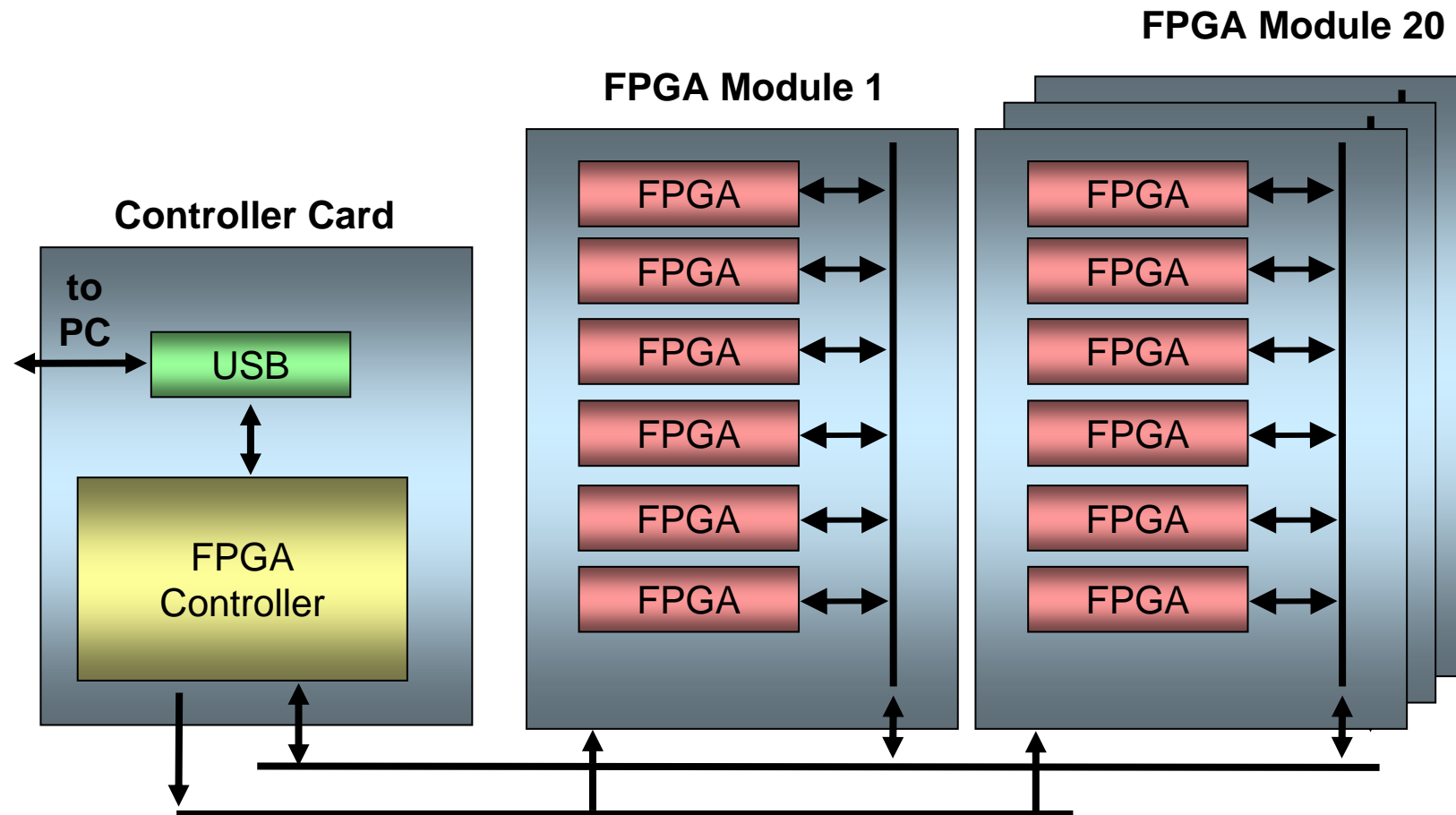


COPACOBANA: Overview

- Currently optimized for DES
- 480 pipelined DES engines (120 FPGAs, 4 DES each)
- Operating at 100 MHz
- Estimated capability
 - 2^{33} Triple DES keys per second
 - a key space of 2^{35} is completely searched in 4 seconds
 - a key space of 2^{40} in 2 minutes



COPACOBANA: Architecture





Conclusion

- Global tracking of e-passport holders is a real threat
- We introduced a system architecture consisting of RF eavesdropper and MRTD cracker
- Security and privacy of citizens must be protected when carrying and using e-passports
 - RFID technology in this context must realize privacy laws
 - All basic principles of data protection law have to be observed when designing, implementing and using RFID technology (see Marc Langheinrich's talk)
 - Further technical discussion need regarding security evaluation (protocols), maintenance (PKI issues, trust relations/models) and future changes
- Many issues are still unclear or confusing
 - Some protection measures are optional
 - Issuing states still did not increase entropy of Basic Access Control Keys
 - Passport still valid even if chip is defect
 - New players, their role and security of their work flows are not thoroughly analyzed
 - Public debate on this important issue has come too short
- What is the choice for citizens to protect their privacy?



Further Work

- Extending operation range of RFID eavesdropper
- Performance analysis of implementation choices for MRTD Cracker
 - e.g., optimizing COPACOBANA to be an efficient MRTD cracker
- Encourage more joint work with security experts, researchers and governmental organisations
 - Thorough and public security analysis of cryptographic components and work flows