BUSLab

Brno University Security Laboratory

Petr Švenda
svenda@fi.muni.cz
Masaryk University, Brno, Czech Rep.

White-box attack resistant cryptography – mobility tickets

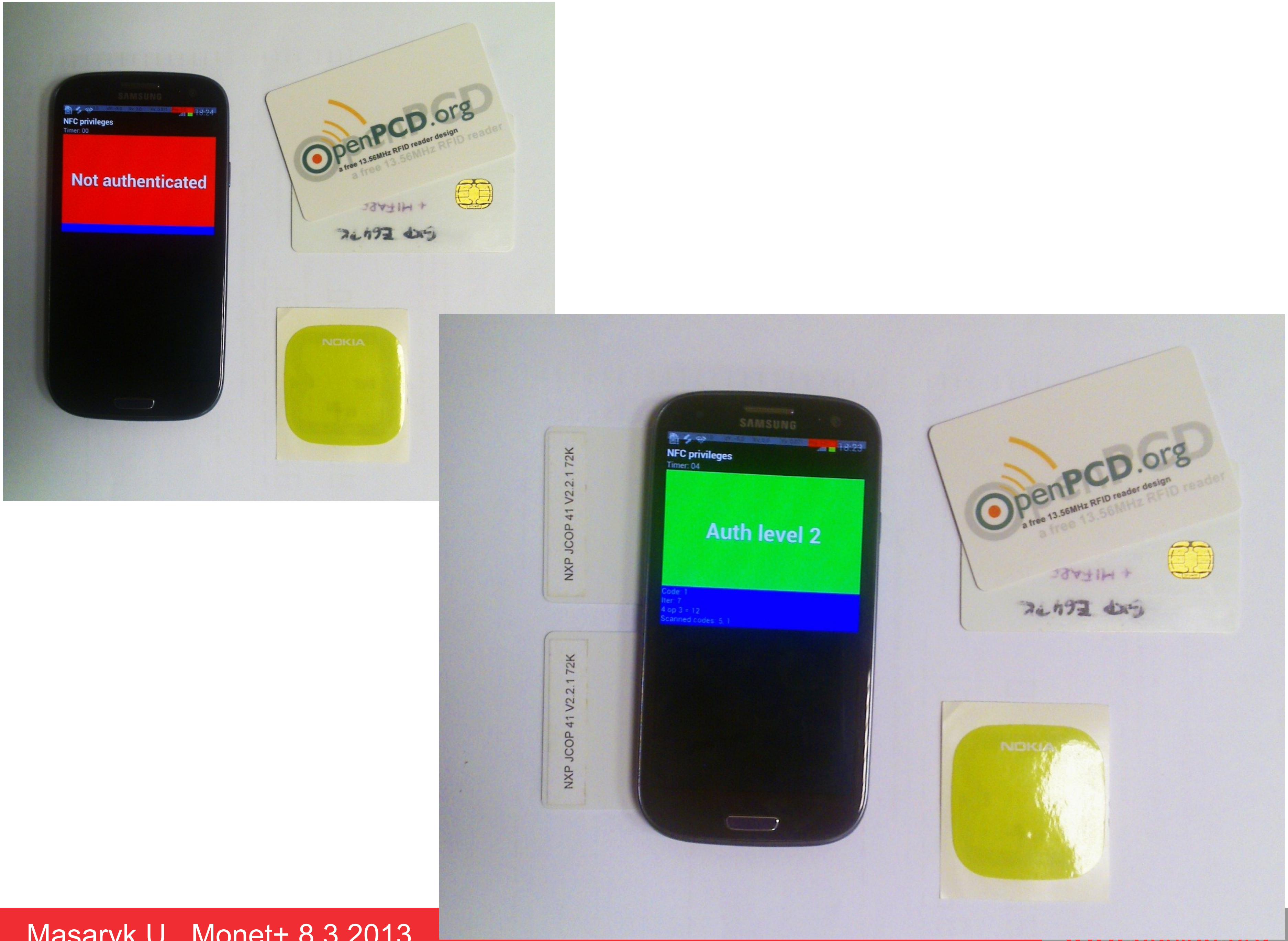
evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Replace smart card by whitebox transform?

- Only to limited extent
- Limitation of arguments size
- Operation atomicity
  - one cannot execute only half of card’s operations
- No secure memory storage
  - no secure update of state (counter)
- Both can be used as black-box
  - smart card can use PIN
- But still some reasonable usages remain

Proximity-based credentials control

- Gradual authorization/credential as opposed to nothing × PIN
- Mobile phone (Android) with NFC reader
- Credentials with different level of sensitivity
  - available based on proximity (NFC) of tags/SC
  - E.g., ISO/IEC 14443 smart cards
- Prototype implemented
  - three levels of control ~ 0, 1 or 2 cards in proximity
  - cryptographic key read from smart card ()
  - GalaxyS3 + JCOP 4.1
  - Application screen reacts to new cards


SAMSUNG
NFC privileges
Timer: 00
Not authenticated
OpenPCD.org
a free 13.56MHz RFID reader design
+ MIFARE
NOKIA
NXP JCOP 41 V2.2.1 72K
NXP JCOP 41 V2.2.1 72K
SAMSUNG
NFC privileges
Timer: 04
Auth level 2
Code: 1
Iter: 7
4 op 3 = 12
Scanned codes: 5, 1
OpenPCD.org
a free 13.56MHz RFID reader design
+ MIFARE
NOKIA

Demo – Android + NFC + SC

- Phone used: Galaxy S3, Android, NFC
  - android.nfc.* (TagViewerPrivileges.java)
- Cards used:
  - JCOP 4.1 with simple JavaCard applet
    - multiply two numbers send via APDU
  - Mifare 1K, Nokia NFC tag…
  - Card with “unknown” ATR (“attacker’s” card)
- Only one card managed by NFC stack at time
  - solved by adding time window

Possible directions

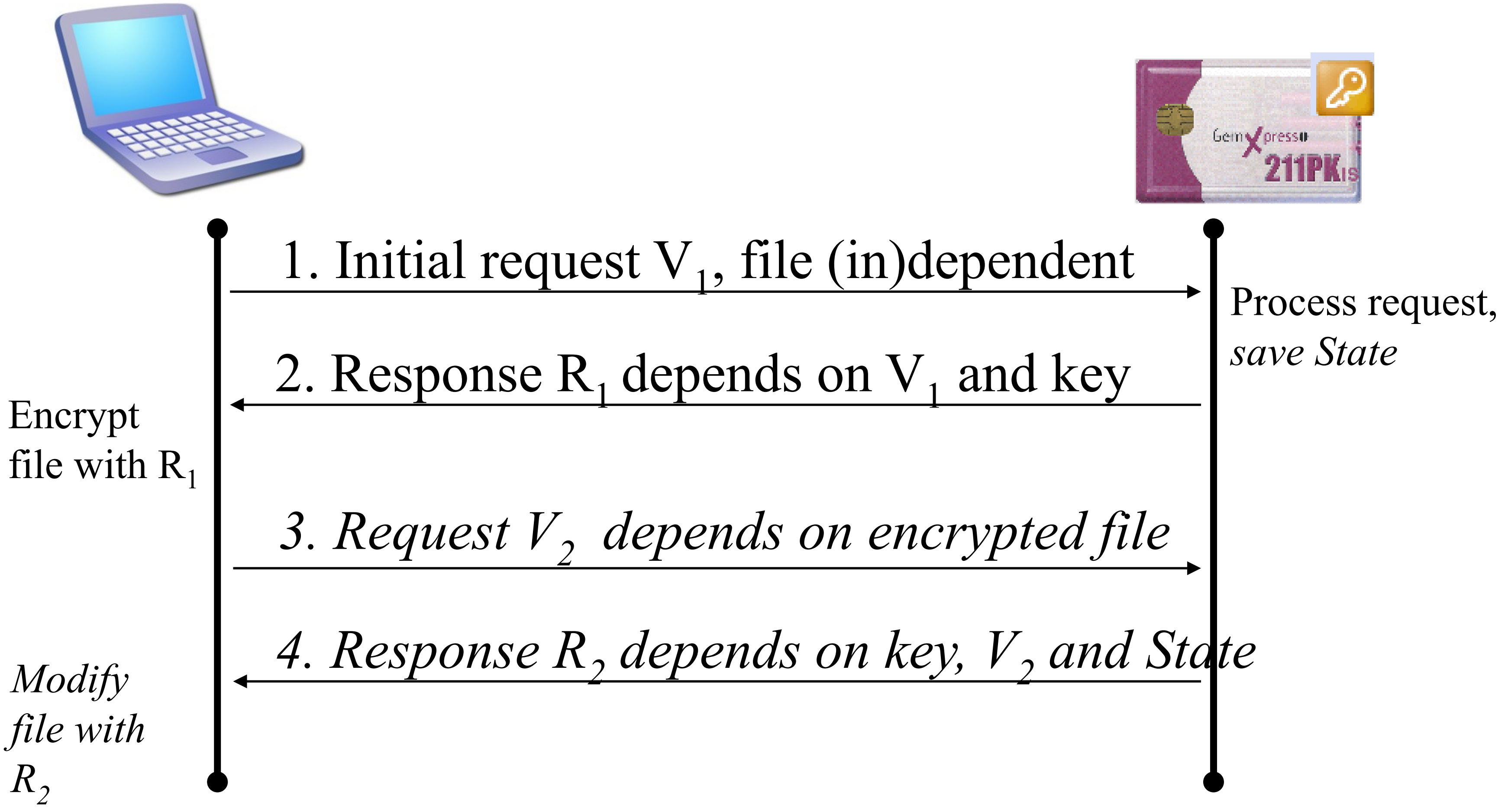
- Card presence (multiple)
- Card presence + key transfer
- Card presence + on-card key usage (operation)
- Card presence + on-card key usage + CEF/CED

- Remotely Keyed Encryption (RKE)?

RKE – requirements, idea

- Requirements:
  - high speed encryption
  - key never leaves smart card
  - encryption/decryption is possible only when smart card is present
- Idea: use on-card encryption, but move heavy work to PC in secure way
  - Remotely Keyed Encryption (Blaze 1996)

RKE call diagram



1. Initial request V_1, file (in)dependent

Process request, *save State*

2. Response R_1 depends on V_1 and key

Encrypt file with R_1

3. Request V_2 depends on encrypted file

4. Response R_2 depends on key, V_2 and State

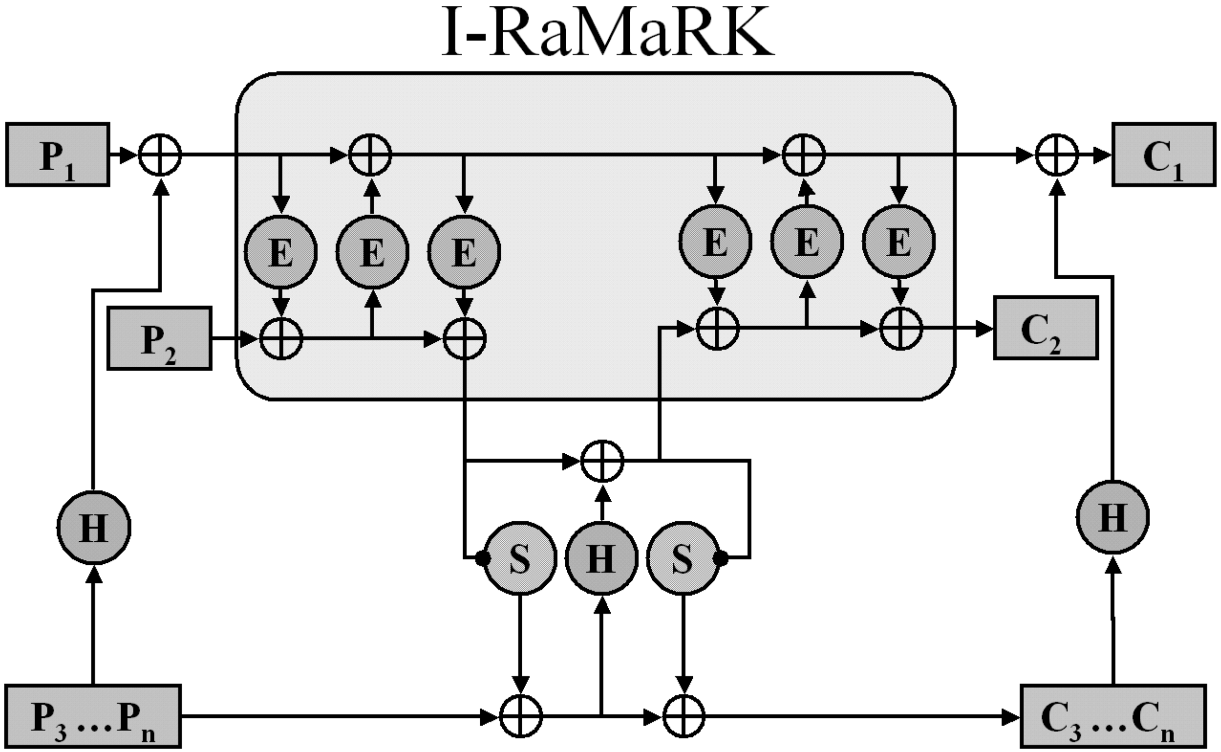
Modify file with R_2

Attacker models

- Basic model (Blaze 96)
  - attacker have no access to SC
  - cannot create own requests
  - attacker completely control PC (ops, values)
- Strong BFN model (BFN 98)
  - attacker had access to SC for limited time
  - was able to create own request (database)
  - no access now

I-RaMaRK

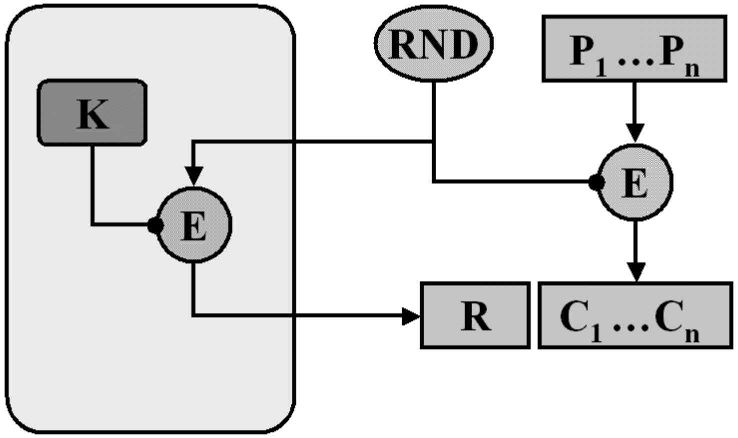
- First secure mode for RKE (strong model)
- Requires 2 APDU messages



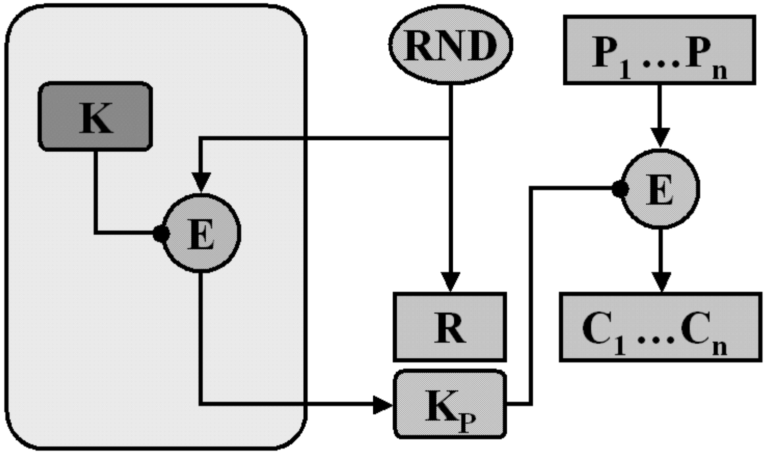
I1 and THCEP

- Fast modes for basic attacker model
  - not inversion/forgery secure, key independent of file
- Requires only 1 APDU message

I1



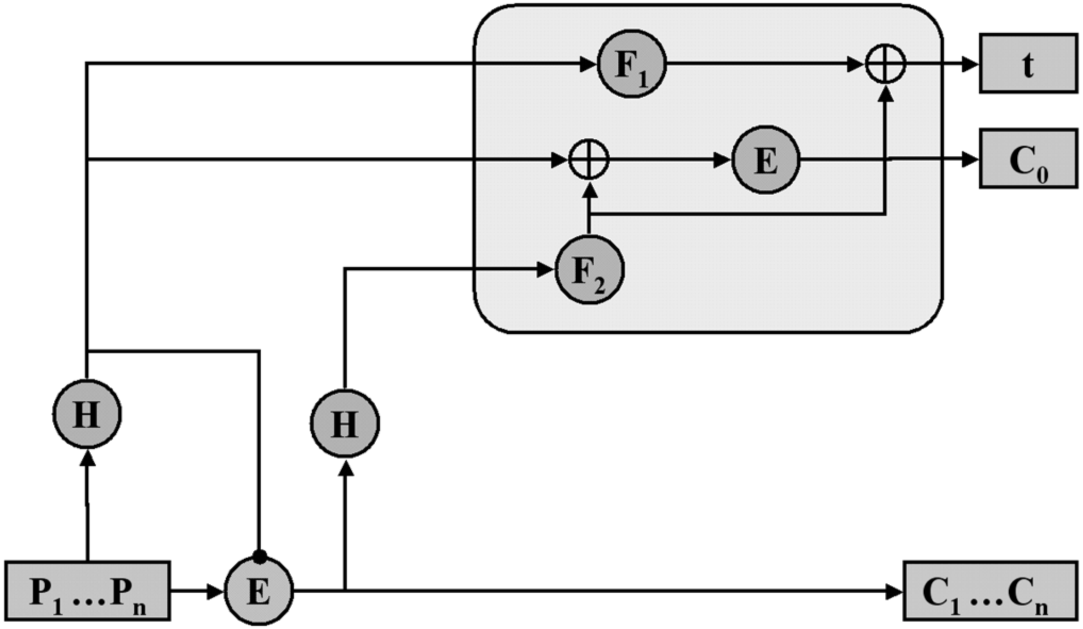
THCEP



Length-Increasing RKE

- 1 APDU mode for strong attacker model
  - randomization nonce must be used

LI-SRKE



Automatic white-box code transformation

- Parse existing source code
- Identify “transformable” operations
  - suitable size of operands
  - no side effects
  - …
- Transform operations into white-box representation
- Or move to smart card
- Update existing code accordingly

Summary

- Homomorphic encryption
  - Presentation only, no real R&D expectations
- Whitebox crypto
  - Implementation of selected schemes planned, open-source
  - Replacement for smartcards?
    - Remotely-keyed encryption
- Proximity-based authorization/credential control
  - Master thesis, proof-of-concept