Research behind smart cards

http://crcs.cz/sc

Petr Švenda svenda@fi.muni.cz
Faculty of Informatics, Masaryk University

CROCS
Centre for Research on Cryptography and Security

Some history

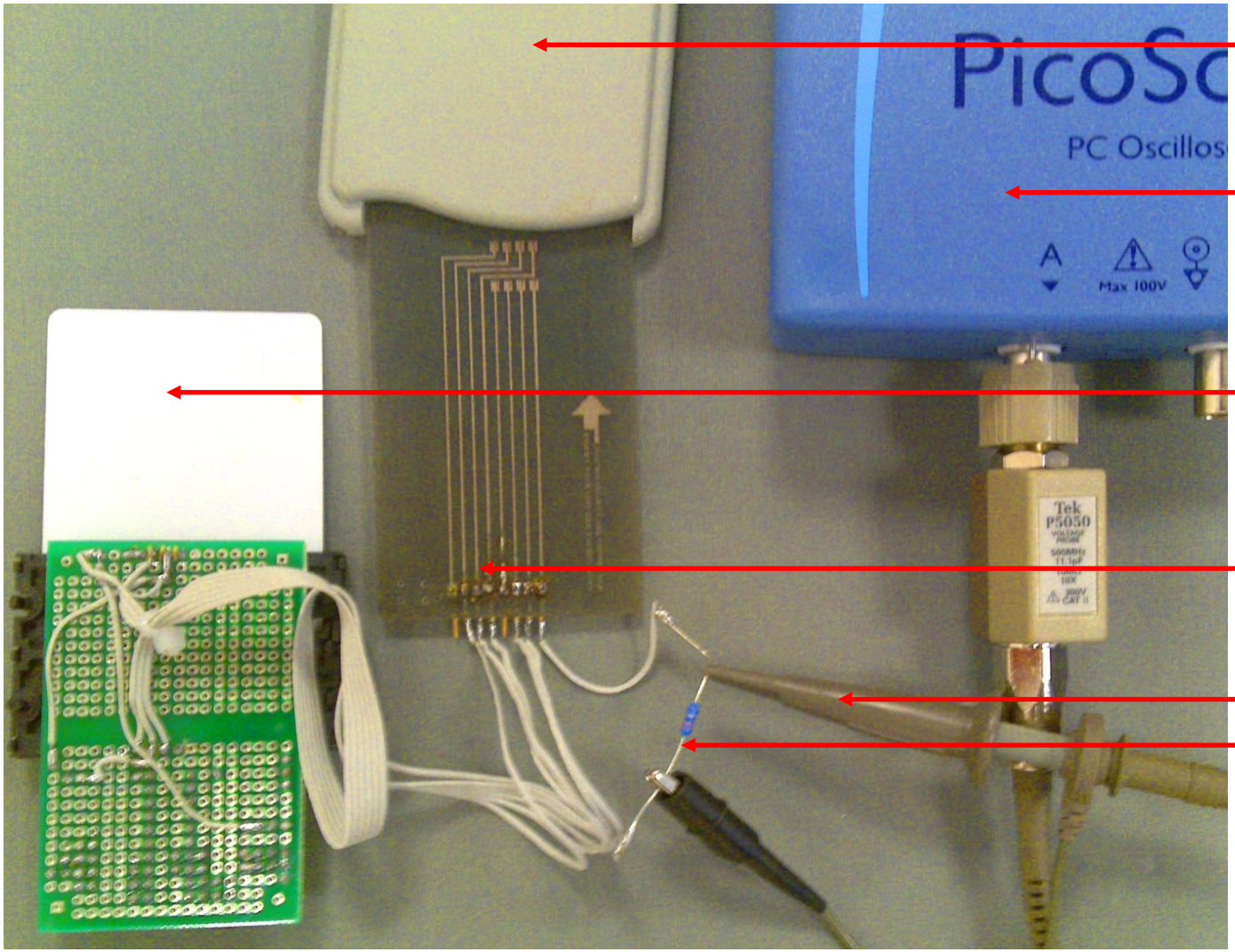
- 2002 – 2009 Cooperation with NBÚ
  - Various topics, main focus on security of smartcards
  - Power analysis with custom boards (SCSAT02/04)
  - On-card TRNG verification (NIST, Diehard)
  - Mostly unpublished research
- 2008-now
  - Security of ePassports
  - JavaCard source code analysis and transformation
  - Capabilities of JavaCards (DB of supported algs, perf)
  - Advanced card applications (AN.ON log, travel cards…)
  - Smart cards + NFC + mobile phones

POWER ANALYSIS

Cryptographic Hardware Security

- Projects focus
  - How to select most suitable smart card?
  - How to test large batch for same hardware?
  - How to detect potential backdoor?
  - How to fix problems with hardware in software?
  - How to let user to confirm transcation amount?
  - Source code audits

Basic setup for power analysis



Smart card reader

Oscilloscope

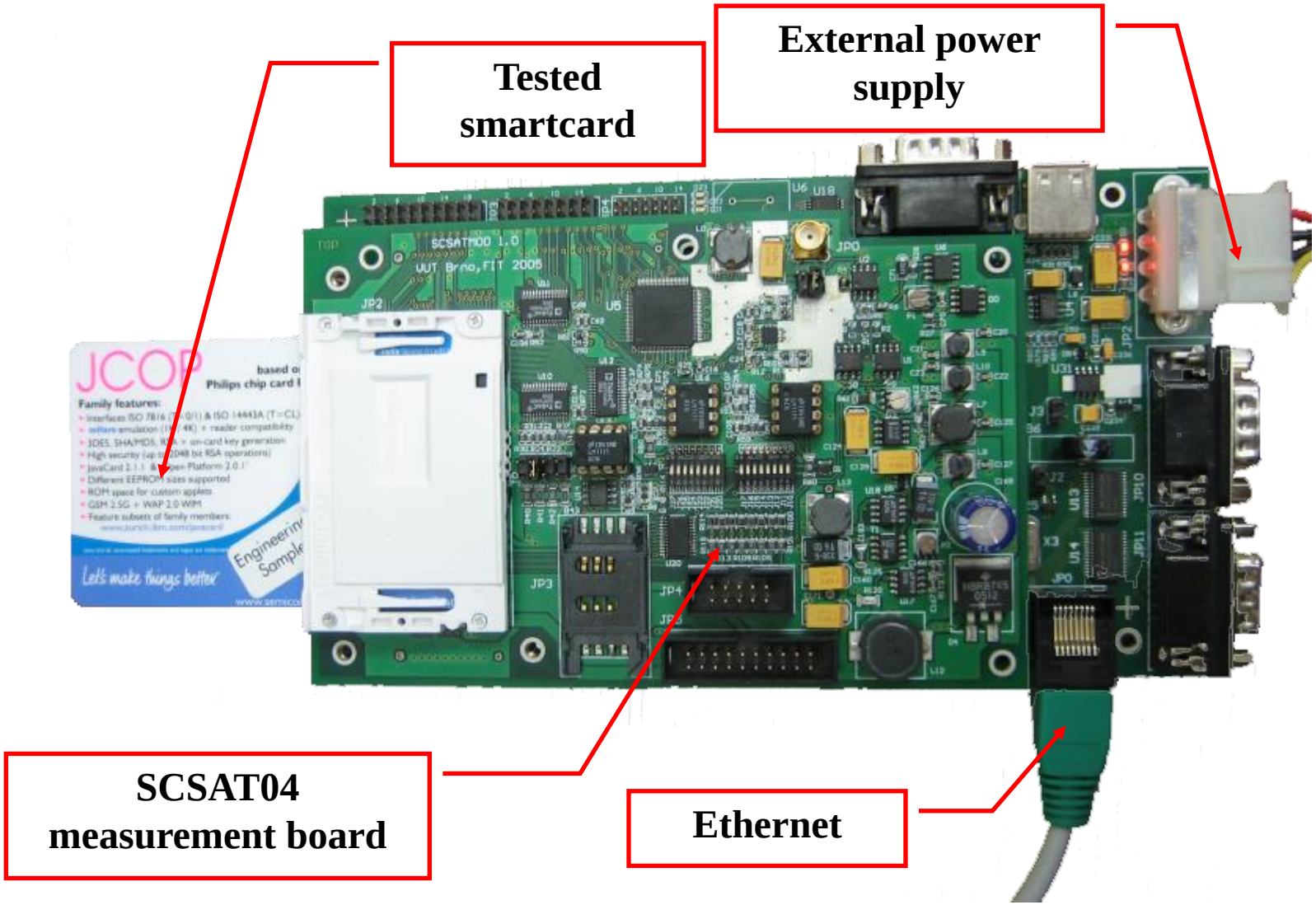
Smart card

Inverse card connector

Probe

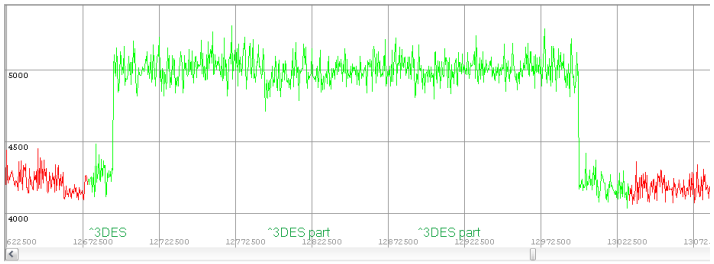
Resistor 20-80 ohm

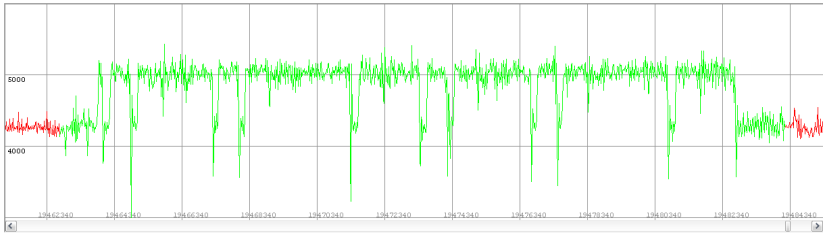
More advanced setup for power analysis

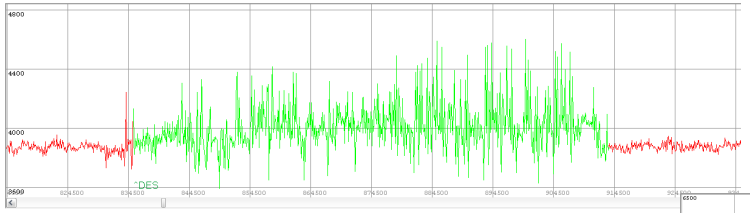


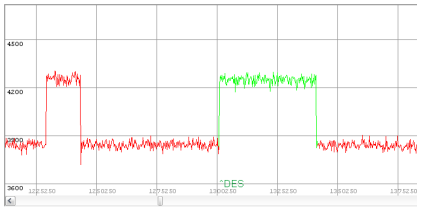
Database of common operations

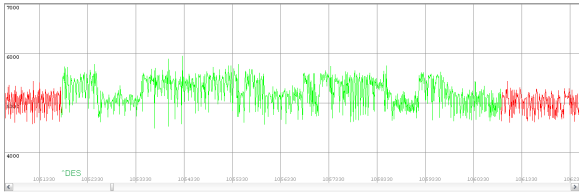
- Power trace of DES, AES, EEPROM, write RAM, RSA, MD5, SHA1/SHA256 …
- GlobalPlatform SCP’0x, PIN verification…

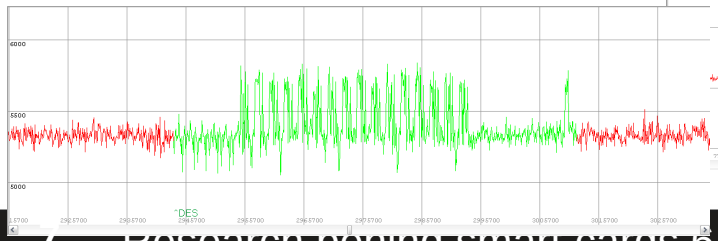


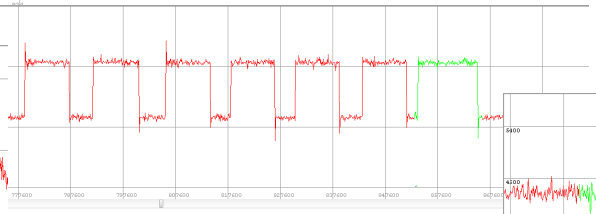


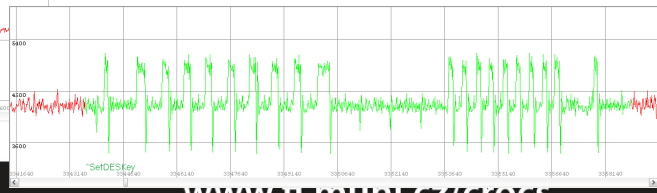






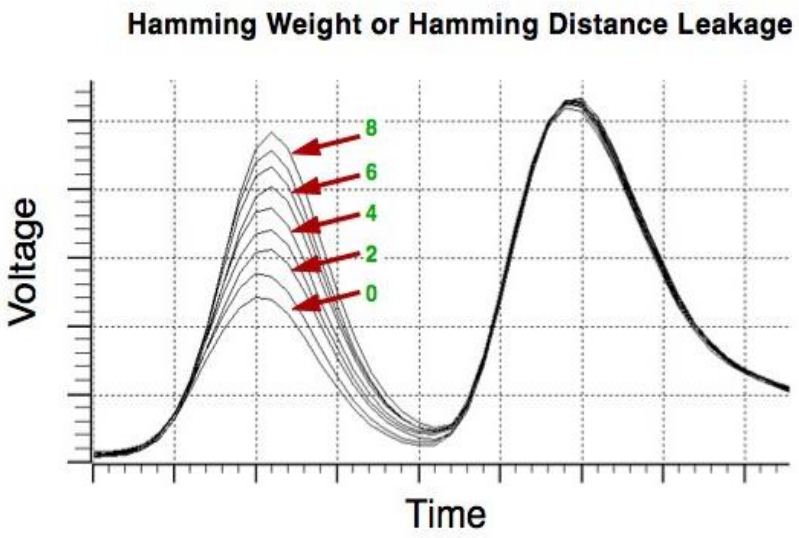






Simple power analysis

```
bool bSimilar = TRUE;
for (short i=0; i<passLength;i++) {
    if (array1[i] != array2[i])
        bSimilar = FALSE;
}
```




```
getfield_a_this 20;
sload_3;
baload;
getfield_a_this 21;
sload_3;
baload;
if_scmpeq L4;
```

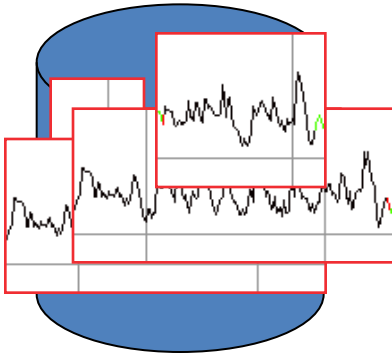
	P	A	S	S	W	O	R	D
array1	P	A	S	S	W	O	R	D
array2	A	B	C	D	E	F	G	H

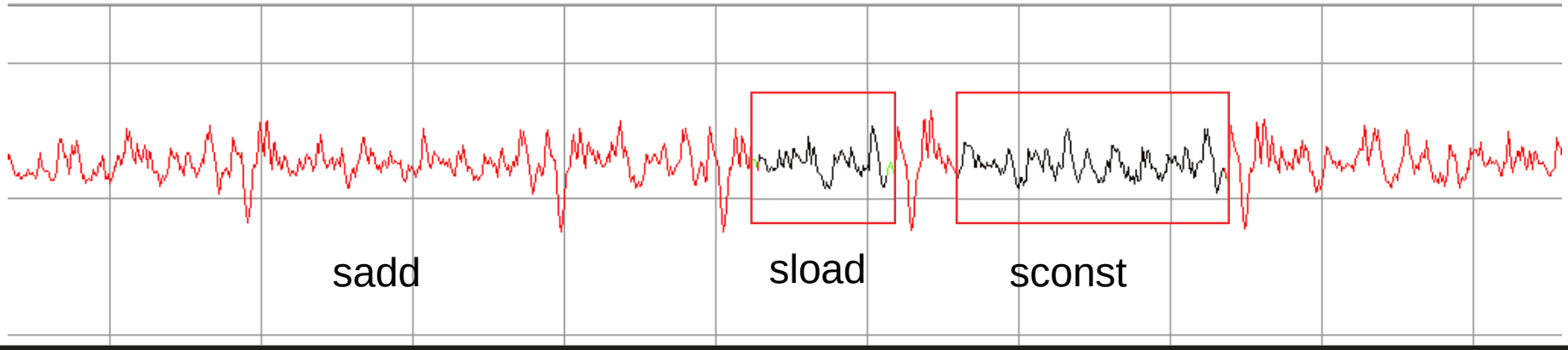
Reverse engineering

Target card

sadd;
unknown;
sload
sconst

sadd;
sstore 4;
sload 4;
sconst_1;
aload_1;
sload 4;





Conditional jumps

- may reveal sensitive info
- keys, internal branches…

(source code)

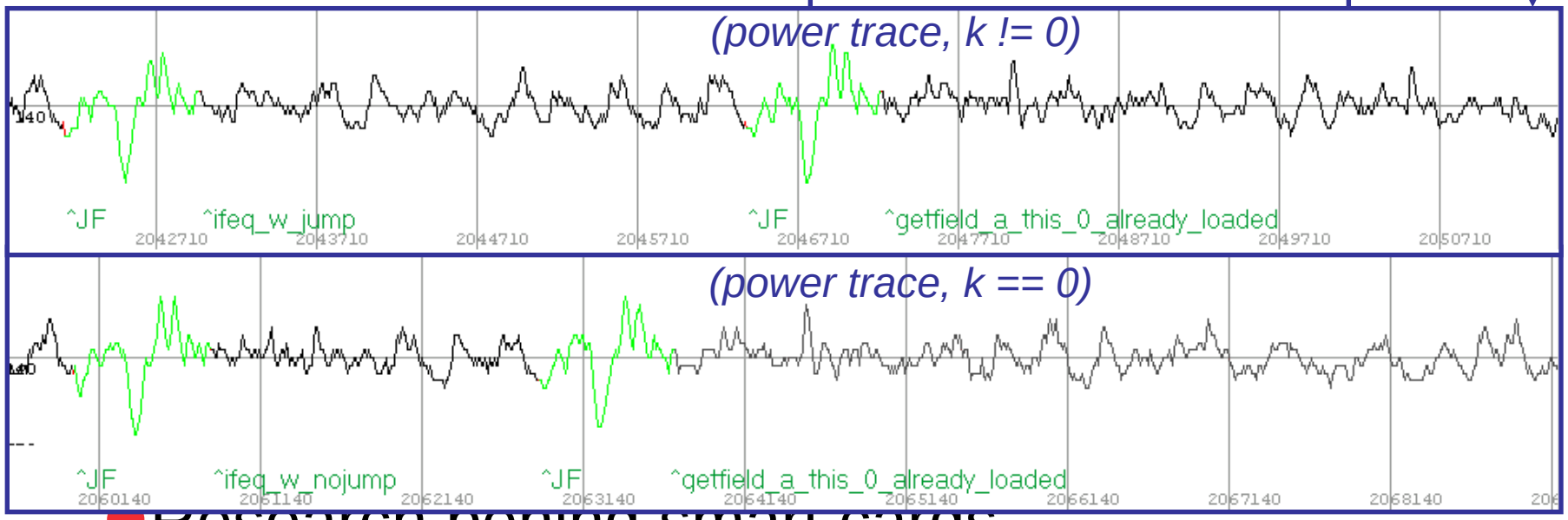
```
if (key == 0) m_ram1[0] = 1;
else m_ram1[0] = 0;
```

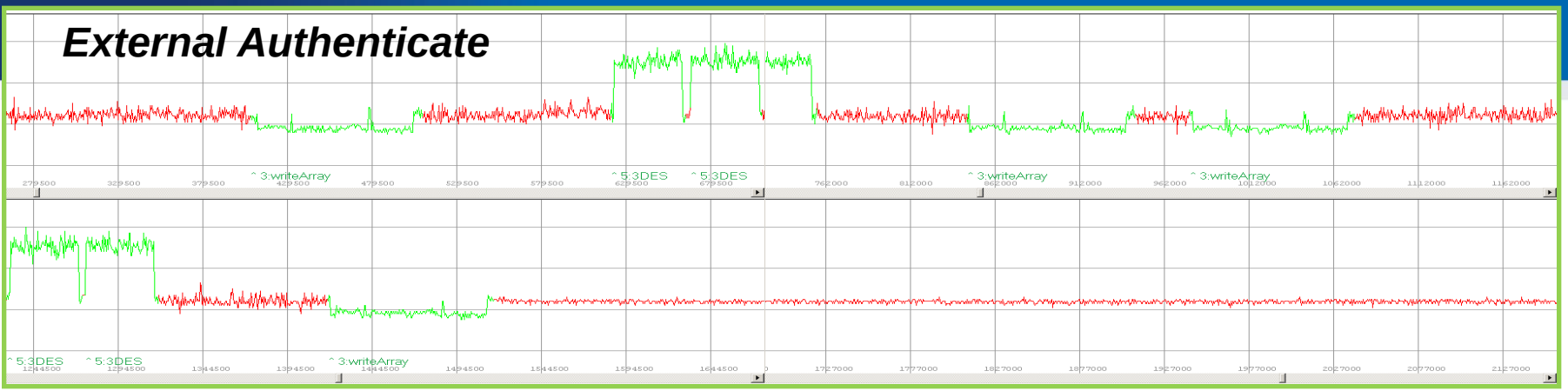
compiler

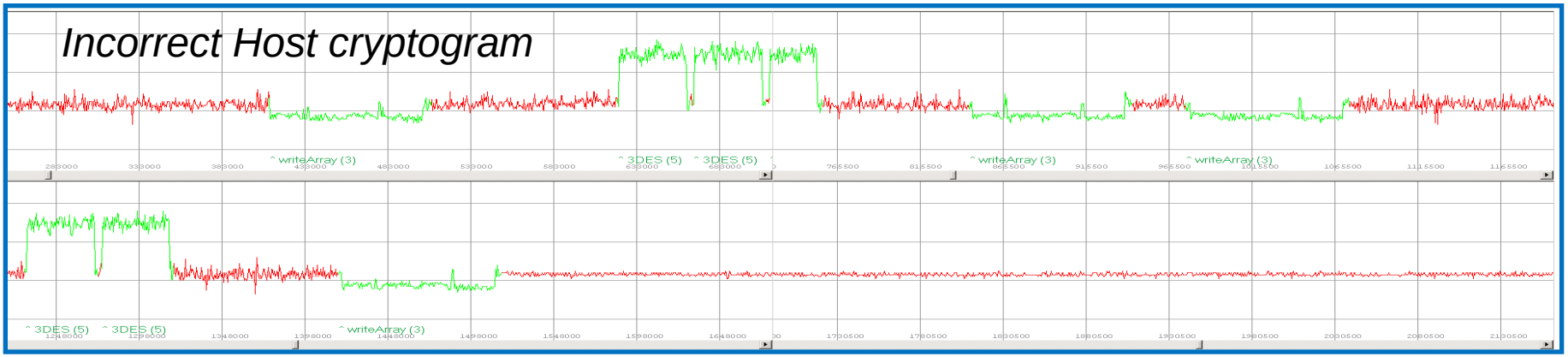
(bytecode)

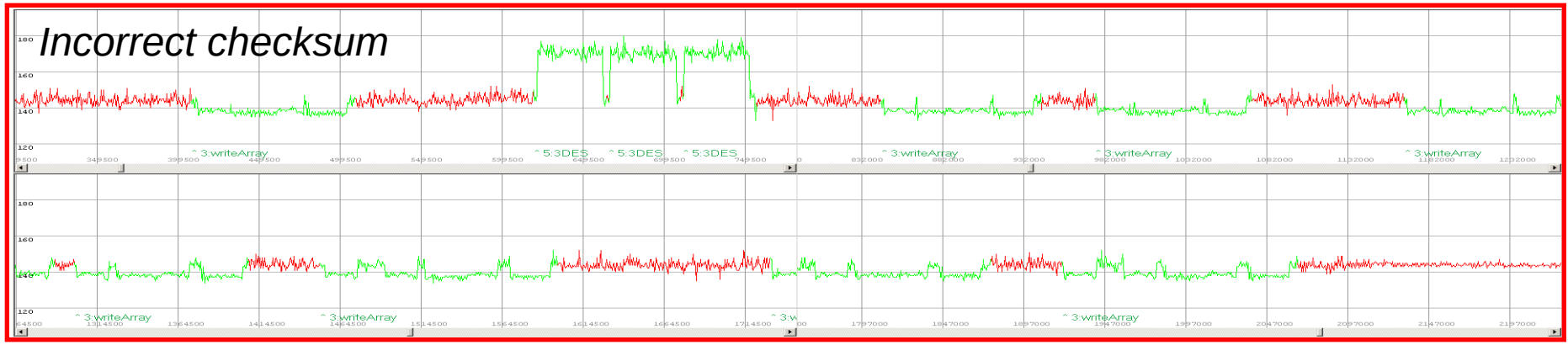
```
     sload_1;
     ifeq_w L2;
L1:  getfield_a_this 0;
     sconst_0;
     sconst_0;
     bastore;
     goto L3;
L2:  getfield_a_this 0;
     sconst_0;
     sconst_1;
     bastore;
     goto L3;
L3:  …
```

oscilloscope




External Authenticate
^ 3:writeArray
^ 5:3DES
^ 5:3DES
^ 3:writeArray
^ 3:writeArray
^ 5:3DES
^ 5:3DES
^ 3:writeArray


Incorrect Host cryptogram
^ writeArray (3)
^ 3DES (5)
^ 3DES (5)
^ writeArray (3)
^ writeArray (3)
^ 3DES (5)
^ 3DES (5)
^ writeArray (3)


Incorrect checksum
^ 3:writeArray
^ 5:3DES
^ 5:3DES
^ 5:3DES
^ 3:writeArray
^ 3:writeArray
^ 3:writeArray
^ 3:writeArray
^ 3:writeArray
^ 3:writeArray

PowerTraceSimulator (PTS) project

- Differential power analysis
  - Gather thousands of traces for different plaintext
  - Use statistical methods to recover bytes of secret key
- Hard to obtain with current smart cards
- PTS provides simulated traces (Rudolf Kvašňovský)
  - Testing of various approaches
  - Educational usage
  - https://github.com/petrs/PowerTraceSimulator

Open topics

- Try new and better PicoScope osci we have now
- Generate and publish public database of common operations for selected cards
  - RNG, AES, RSA, ECC…
- …

ON-CARD RSA KEYS

Verifying of on-card key generation

- On-card key generation functionality
- Up to RSA-2048 bits keys
- RNG → prime(s) → RSA key
- Keys seems to be random…

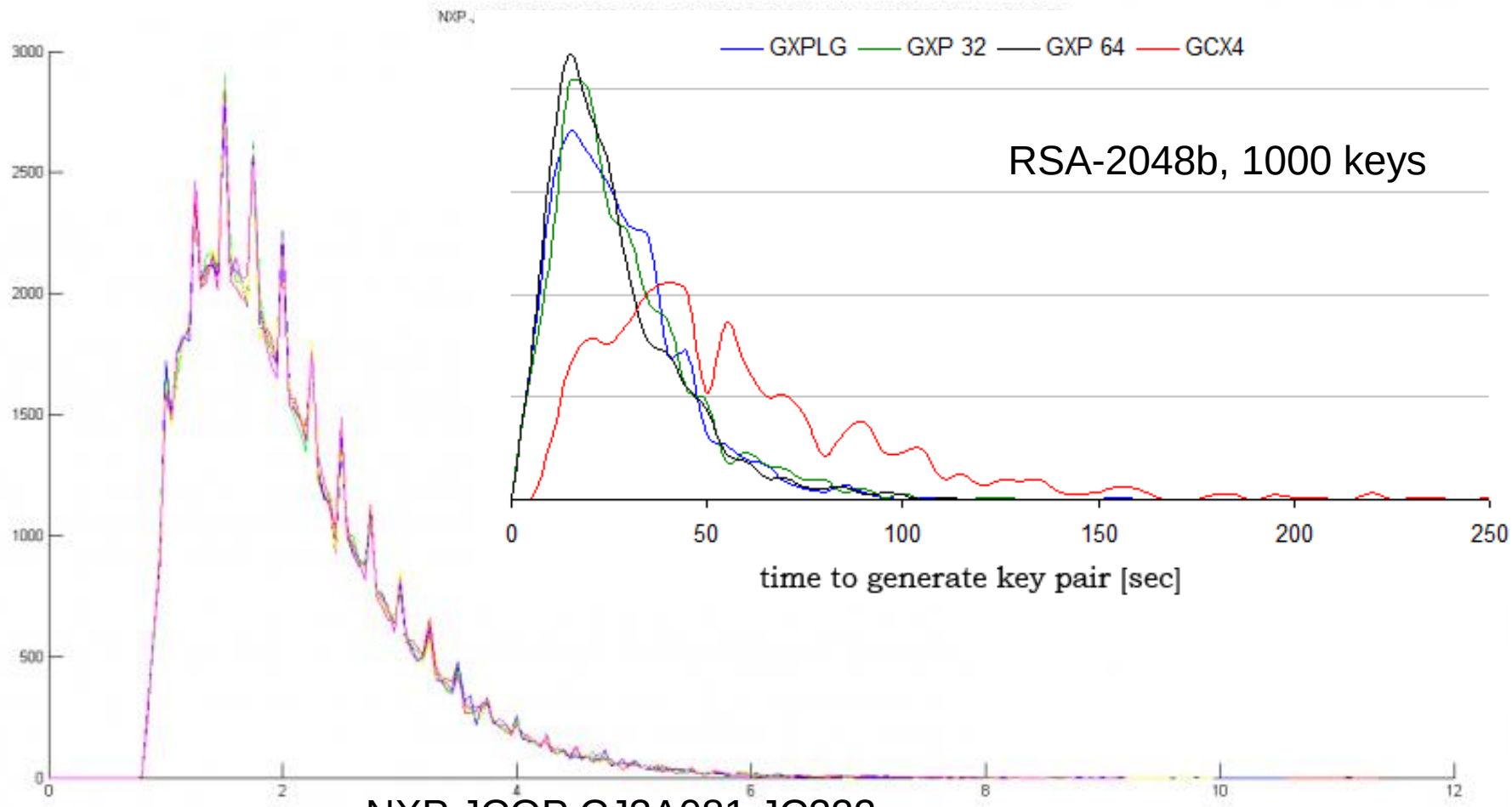
```
PUBL: 82 00 03 01 00 01 82 00 80 c6 84 74 12 8c cd 64 fc 92 2e
PRIV: 82 00 40 cf 36 3e 0e 0b 3f 31 c9 ca e7 ac 72 ff db 85 59
# 1:7.941

PUBL: 82 00 03 01 00 01 82 00 80 bb ce 53 0b d0 1a b3 e6 e4 18
PRIV: 82 00 40 c7 e6 94 29 50 45 31 53 f6 16 59 57 0e 1e 89 06
# 2:3.842
```

…

How to gather 100 000+ key pairs?

Histogram of on-card generation time



NXP JCOP CJ3A081 JC222

Analysis

- Analysis of RSA keys generated on smartcards (David Formánek)
  - Wiener's attack for small private exponents
  - Possibility of module factorization
  - Frequency distribution of primes in keys
  - Next prime predictability
- Keycheck tool https://github.com/formanek/keycheck
  - Interesting deviances found!

Open topics

- Gather more keys from more cards
- More RSA keys tests and especially interpretation
- ECC keys
- …

JCALGTESTER

Problem?

What kind of smart card?

How much RAM memory?

Which algorithms supported?

Which one should I choose?

What key lengths?

How much persistent memory?

What version of JavaCard API?

JavaCard AlgTester - 2009

```
try {
  m_cipher = Cipher.getInstance(ALG_DES_CBC_NOPAD, false);
  // If this line is reached, than DES in CBC mode with no padding
  // (ALG_DES_CBC_NOPAD) is supported.
  supported = true;
} catch (CryptoException e) {
  if (e.getReason() == CryptoException.NO_SUCH_ALGORITHM)) {
  // algorithm is not supported
  supported = false;
} else { // other error occured
```

Tested cards abbreviations:
c1 Oberthur Cosmo Dual 72K 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00
c2 Gemplus GCX4 72k PK (GemCombiXpresso + integrated Mifare1k), 3B:7A:94:00:00:80:65:A2:01:01:01:3D:72:D6:43
c3 NXP JCOP 4.1 V2.2.1, 3B:FA:18:00:00:81:31:FE:45:4A:43:4F:50:34:31:56:32:32:31:9D
c4 NXP JCOP31 V2.2 36K 3B:EB:00:00:81:31:20:45:4A:43:4F:50:33:31:33:36:47:44:54:78
c5 Gemalto GXP R4 72K (TOP IM GX4), 3B:7D:94:00:00:80:31:80:65:B0:83:11:C0:A9:83:00:90:00
c6 Gemplus GXP Pro-R3.2 (TOP IS GX3) 3B:7D:94:00:00:80:31:80:65:B0:83:01:02:90:83:00:90:00
c7 Gemplus GXPPro-R3 3B:7B:94:00:00:80:65:B0:83:01:01:74:83:00:90:00
c8 Gemplus GXPLite-Generic 3B:7D:94:00:00:80:31:80:65:B0:83:01:02:90:83:00:90:00
c9 Gemplus GXP E64 PK (TOP IM GX3) 3B:7E:94:00:00:80:25:A0:00:00:00:28:56:80:10:21:00:01:08
c10 Axalto Cyberflex Palmera V5 3B:E6:00:00:81:21:45:32:4B:01:01:01:01:7A
c11 Schlumberger Cyberflex 32K e-gate: ATR = 3B 75 94 00 00 62 02 02 02 01
c12 Nokia 6131 phone, ATR = 3B:88:80:01:00:73:C8:40:13:00:90:00:71

Note: Blank white box means that algorithm was not tested yet with the card and will be added in future. Error means that tested card gives permanent error other then CryptoException.NO_SUCH_ALGORITHM when called.

javacardx.crypto.Cipher	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11	c12
ALG_DES_CBC_NOPAD	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	Yes
ALG_DES_CBC_ISO9797_M1	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	Yes
ALG_DES_CBC_ISO9797_M2	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	yes
ALG_DES_CBC_PKCS5	no	no	no	no	no	no	no	no	no	no	no	yes
ALG_DES_ECB_NOPAD	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
ALG_DES_ECB_ISO9797_M1	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	yes

JavaCard AlgTester - 2012

- New Java parsing client (AlgTestJClient)
- Additional platform information parsed (JCSystem())
- Added speed testing for selected algorithms
- RSA-based modular exponentiation hack testing added

Tested cards abbreviations:
c1 Oberthur Cosmo Dual 72K 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00
c2 Gemplus GCX4 72k PK (GemCombiXpresso + integrated Mifare1k), 3B:7A:94:00:00:80:65:A2:01:01:01:3D:72:D6:43
c3 NXP JCOP 4.1 V2.2.1, 3B:FA:18:00:00:81:31:FE:45:4A:43:4F:50:34:31:56:32:32:31:9D
c4 NXP JCOP31 V2.2 36K 3B:EB:00:00:81:31:20:45:4A:43:4F:50:33:31:33:36:47:44:54:78
c5 Gemalto GXP R4 72K (TOP IM GX4), 3B:7D:94:00:00:80:31:80:65:B0:83:11:C0:A9:83:00:90:00
c6 Gemplus GXP Pro-R3.2 (TOP IS GX3) 3B:7D:94:00:00:80:31:80:65:B0:83:01:02:90:83:00:90:00
c7 Gemplus GXPPro-R3 3B:7B:94:00:00:80:65:B0:83:01:01:74:83:00:90:00
c8 Gemplus GXPLite-Generic 3B:7D:94:00:00:80:31:80:65:B0:83:01:02:90:83:00:90:00
c9 Gemplus GXP E64 PK (TOP IM GX3) 3B:7E:94:00:00:80:25:A0:00:00:00:28:56:80:10:21:00:01:08
c10 Axalto Cyberflex Palmera V5 3B:E6:00:00:81:21:45:32:4B:01:01:01:01:7A
c11 Schlumberger Cyberflex 32K e-gate: ATR = 3B 75 94 00 00 62 02 02 02 01
c12 Nokia 6131 phone, ATR = 3B:88:80:01:00:73:C8:40:13:00:90:00:71

Note: Blank white box means that algorithm was not tested yet with the card and will be added in future. Error means that tested card gives permanent error other then CryptoException.NO_SUCH_ALGORITHM when called.

javacardx.crypto.Cipher	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11	c12
ALG_DES_CBC_NOPAD	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	Yes
ALG_DES_CBC_ISO9797_M1	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	Yes
ALG_DES_CBC_ISO9797_M2	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	yes
ALG_DES_CBC_PKCS5	no	no	no	no	no	no	no	no	no	no	no	yes
ALG_DES_ECB_NOPAD	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
ALG_DES_ECB_ISO9797_M1	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	yes

What's new in 2014? ☺

Lukáš Šrom is on board ☺

Tested cards abbreviations:

c0 Athena IDprotect , ATR=3B D5 18 FF 80 91 FE 1F C3 80 73 C8 21 13 08 (provided by Cosm
c1 Axalto Cyberflex32 , ATR=3B 75 94 00 00 62 02 02 02 01 (provided by PetrS)
c2 Axalto Cyberflex PalmeraV5 , ATR=3B E6 00 00 81 21 45 32 4B 01 01 01 01 7A (provided by PetrS)
c3 G+D SmartCafe Expert 144k Dual , ATR=3b fd 18 00 00 80 31 fe 45 73 66 74 65 20 63 64 31 34 34 2d 6e 66 d8 (provided by Diego NdK)
c4 G+D SmartCafe Expert 3.2 72K , ATR=3B F7 18 00 00 80 31 FE 45 73 66 74 65 2D 6E 66 C4 (provided by Cosmo)
c5 Gemalto IDCore 10 , ATR=3b 7d 96 00 00 80 31 80 65 b0 83 11 d0 a9 83 00 90 00 (provided by Martin Paljak)
c6 Gemalto IDCore 3010 CC , ATR=3b 7d 96 00 00 80 31 80 65 b0 85 02 00 cf 83 01 90 00 (provided by Martin Paljak)
c7 Gemalto TOP IM GXP4 , ATR=3b 7d 94 00 00 80 31 80 65 b0 83 11 d0 a9 83 00 90 00 (provided by PetrS)
c8 Gemalto TwinGCX4 72k PK , ATR=3B 7A 94 00 00 80 65 A2 01 01 01 3D 72 D6 43 (provided by PetrS)
c9 Gemplus GXPE64PK , ATR=3B 7E 94 00 00 80 25 A0 00 00 00 28 56 80 10 21 00 01 08 (provided by PetrS)
c10 Gemplus GXPLiteGeneric , ATR=3B 7D 94 00 00 80 31 80 65 B0 83 01 02 90 83 00 90 00 (provided by PetrS)
c11 Gemplus GXPR3r32 , ATR=3B 7D 94 00 00 80 31 80 65 B0 83 01 02 90 83 00 90 00 (provided by PetrS)
c12 Gemplus GXPR3 , ATR=3B 7B 94 00 00 80 65 B0 83 01 01 74 83 00 90 00 (provided by PetrS)
c13 Infineon JTOPV2 16K , ATR=3B 6D 00 00 80 31 80 65 40 90 86 01 51 83 07 90 00 (provided by PetrS)
c14 Nokia 6131 , ATR=3B 88 80 01 00 73 C8 40 13 00 90 00 71 (provided by Hakan Karahan)
c15 NXP JCOP10 (DES only version) , ATR=3b e9 00 00 81 31 fe 45 4a 43 4f 50 31 30 56 32 32 a3 (provided by Henrik)
c16 NXP JCOP31 , ATR=3B EB 00 00 81 31 20 45 4A 43 4F 50 33 31 33 36 47 44 54 78 (provided by PetrS)
c17 NXP JCOP41 v221 , ATR=3b fa 18 00 00 81 31 fe 45 4a 43 4f 50 34 31 56 32 32 31 9d (provided by PetrS)
c18 NXP JCOP CJ2A081 JC222 , ATR=3b f8 18 00 ff 81 31 fe 45 4a 43 4f 50 76 32 34 31 43 (provided by PetrS)
c19 NXP JCOP CJ3A080v241 , ATR=3B F8 13 00 00 81 31 FE 45 4A 43 4F 50 76 32 34 31 B7 (provided by Lazuardi Nasution)
c20 NXP JCOP CJ3A081 JC222 , ATR=3b fa 18 00 00 81 31 fe 45 4a 33 41 30 38 31 56 32 34 31 89 (provided by PetrS)
c21 NXP JCOP J2A080 , ATR=3b f6 18 00 ff 81 31 fe 45 4a 32 41 30 38 30 1b (provided by Pierre-d)
c22 NXP JCOP J3D081 v242 , ATR=3b f9 13 00 00 81 31 fe 45 4a 43 4f 50 32 34 32 52 32 a3 (provided by Martin Paljak)
c23 Oberthur CosmoDual72K , ATR=3B 7B 18 00 00 00 31 C0 64 77 E3 03 00 82 90 00 (provided by PetrS)
c24 Oberthur Cosmo V7 64K Dual 128K , ATR=3B DB 18 00 80 B1 FE 45 1F 83 00 31 C0 64 C7 FC 10 00 01 90 00 FA (provided by Cosmo)
c25 Yubikey Neo , ATR=3b fa 13 00 00 81 31 fe 15 59 75 62 69 6b 65 79 4e 45 4f a6 (provided by Pierre-d and Cosmo)
c26 [undisclosed1] , ATR=3b xx xx xx xx xx xx xx xx xx xx xx xx xx xx (provided by Cosmo)
c27 [undisclosed2] , ATR=3b xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx (provided by Cosmo)
c28 [undisclosed3] , ATR=3b xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx (provided by Cosmo)
c29 [undisclosed4] , ATR=3b xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx (provided by Cosmo)

Fork me on GitHub

Current state (and close future)

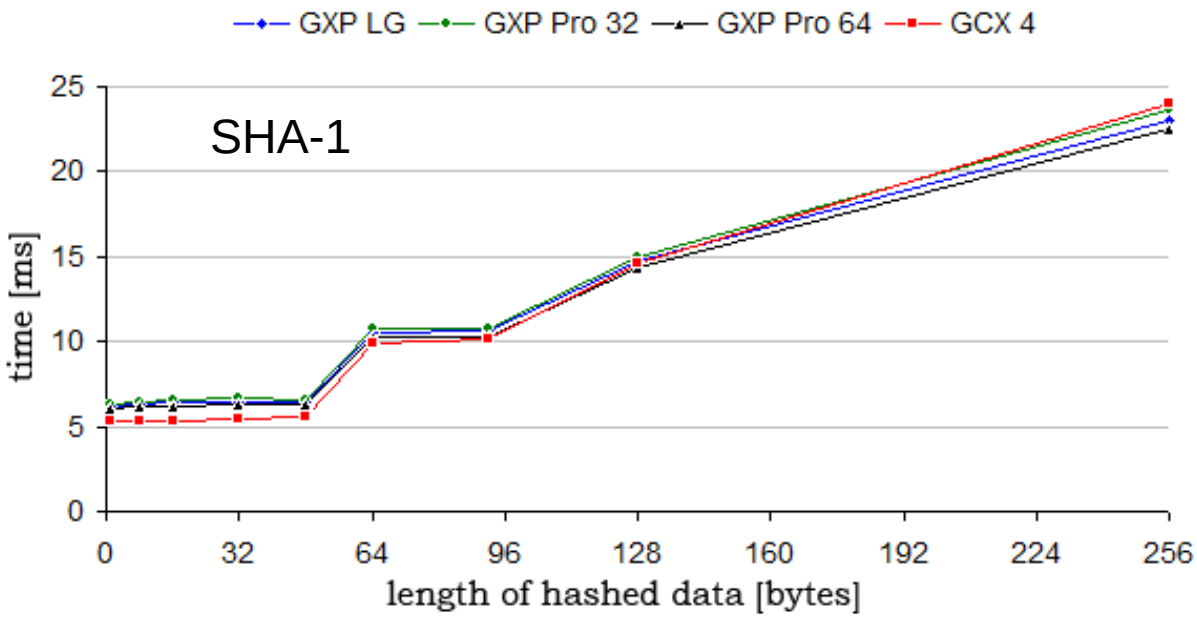
- Testing application for supported algorithms
  - You can obtain information about your smart card
  - https://github.com/petrs/JCAlgTest
- Database of results (31 cards at the moment)
  - Find card you have or you like to have
  - http://www.fi.muni.cz/~xsvenda/jcsupport.html
- Testing application for algorithms performance
  - Generate or find performance graphs
- Power traces for selected algorithms
  - Annotated database of power traces

Card performance testing

- How to
  - Measuring time between APDU (multiple inner iterations)
  - Measuring time directly from power trace
- Almost ready, final cleaning of code and measured results (Lenka Kuníková)
  - Testing applet and processing application
  - Results for cards in our laboratory

Basic crypto - performance

- DES, AES (one block) ~ 3-10ms
- SHA-1/SHA-2 (one block) ~ 3-6ms
- RandomData (16B) ~ 1-5ms



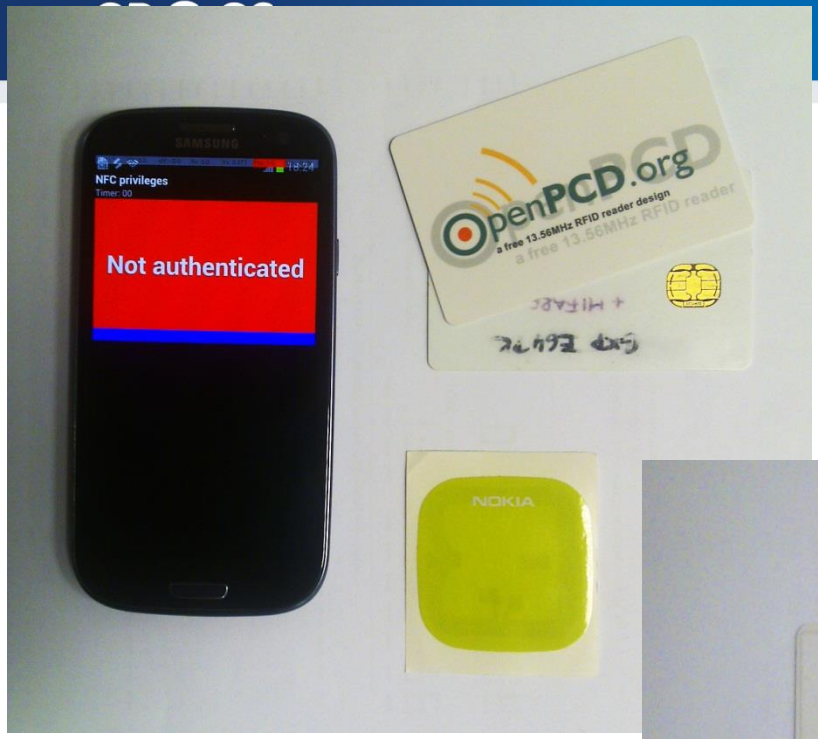
Open topics

- Polish and publish performance testing tool
- Easy submit of results, card fingerprinting server
- Update JavaCard development tutorial
- …

SMART CARDS AND MOBILES

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 (Dušan Klinec)
  - 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
NOKIA

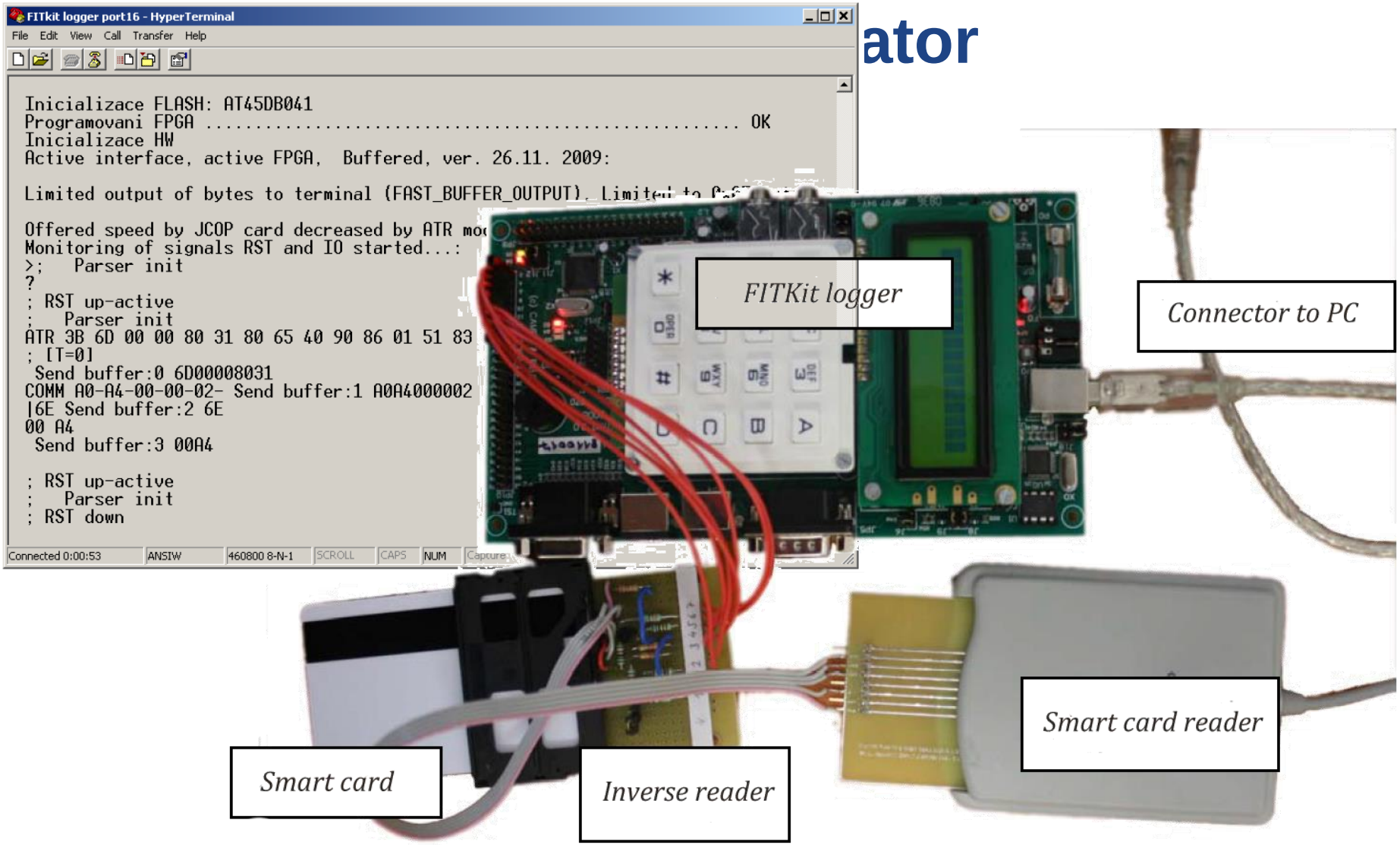

SAMSUNG
NFC privileges
Timer: 04
Auth level 2
Code: 1
Iter: 7
4 op 3 = 12
Scanned codes: 5, 1
NXP JCOP 41 V2.2.1 72K
NXP JCOP 41 V2.2.1 72K
OpenPCD.org
a free 13.56MHz RFID reader design
NOKIA

Open topics

- Analysis of performance of sign operation
  - Various combination of phone + NFC chip + card
- Gathering info from on-board sensors
- Randomness extraction and evaluation
- …

APDU CAPTURE/MANIP

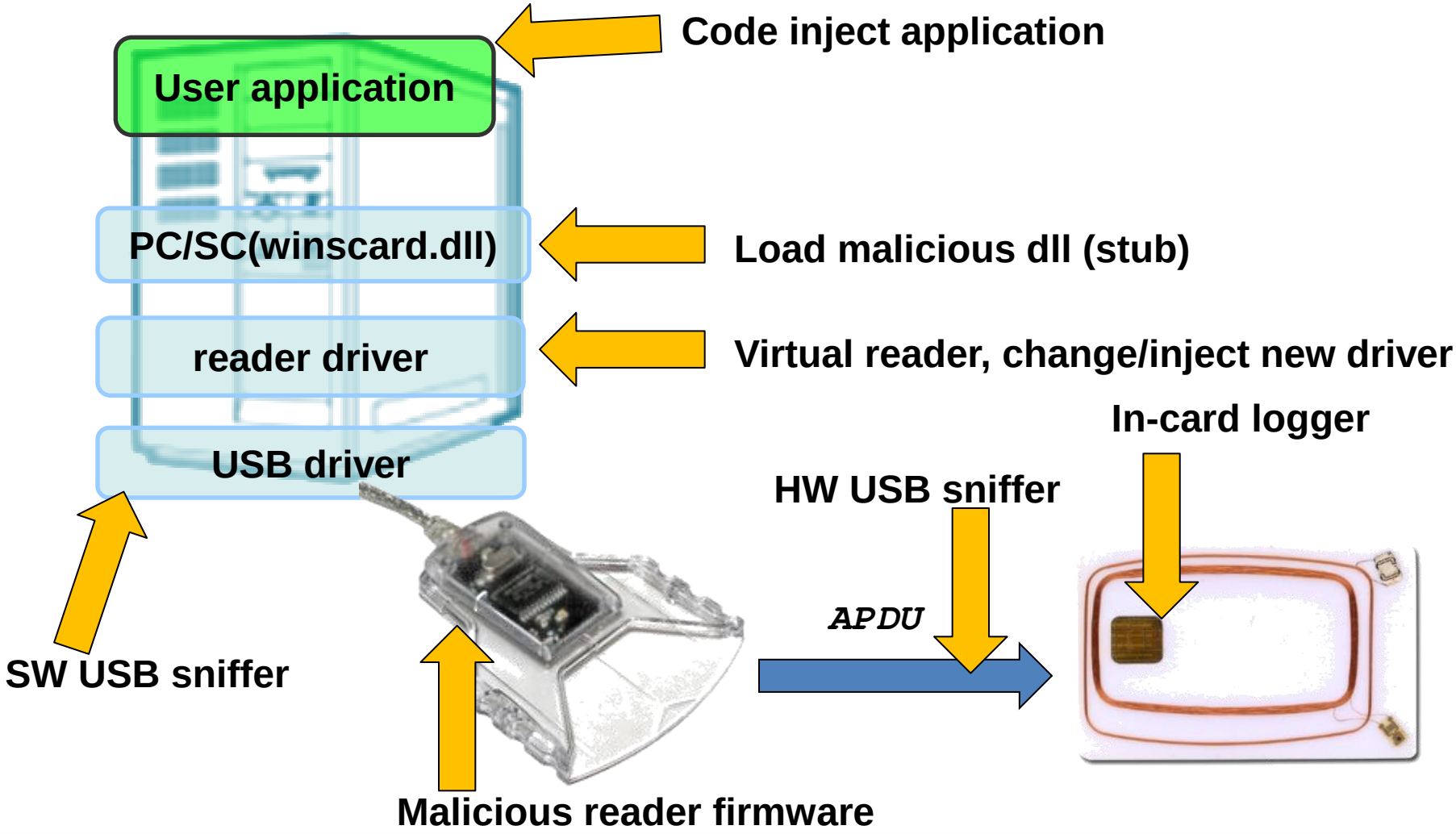
ator


FITKit logger port16 - HyperTerminal
File Edit View Call Transfer Help
Inicializace FLASH: AT45DB041
Programovani FPGA ..... OK
Inicializace HW
Active interface, active FPGA, Buffered, ver. 26.11. 2009:
Limited output of bytes to terminal (FAST_BUFFER_OUTPUT). Limited to
Offered speed by JCOP card decreased by ATR mo
Monitoring of signals RST and IO started...:
>; Parser init
?
; RST up-active
; Parser init
ATR 3B 6D 00 00 80 31 80 65 40 90 86 01 51 83
; [T=0]
Send buffer:0 6D00008031
COMM A0-A4-00-00-02- Send buffer:1 A0A4000002
|6E Send buffer:2 6E
00 A4
Send buffer:3 00A4
; RST up-active
; Parser init
; RST down
Connected 0:00:53
ANSIW
460800 8-N-1
SCROLL
CAPS
NUM
Capture
FITKit logger
Connector to PC
Smart card reader
Smart card
Inverse reader

Proxmark III

- Programmable device capable to simulate various contactless cards/tags
- Man-in-the-middle attack (door access, bezkontatní platby…)
- ePassport simulator (Martin Korec) https://is.muni.cz/auth/th/396490/fi_b/

Where to log/manipulate communication?



Let's write own winscard.dll (PC/SC)

based on ApduView utility (by Fernandes)

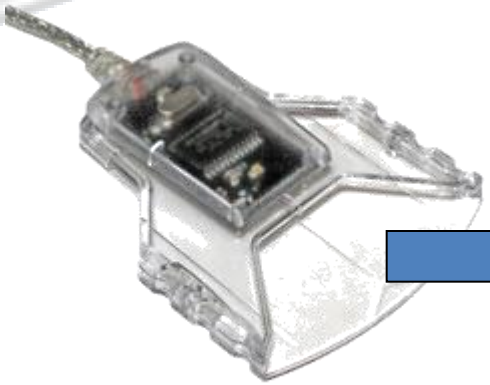
User application

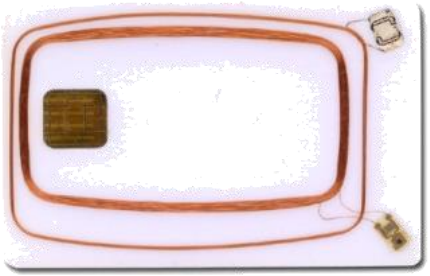
winscard.dll (stub)

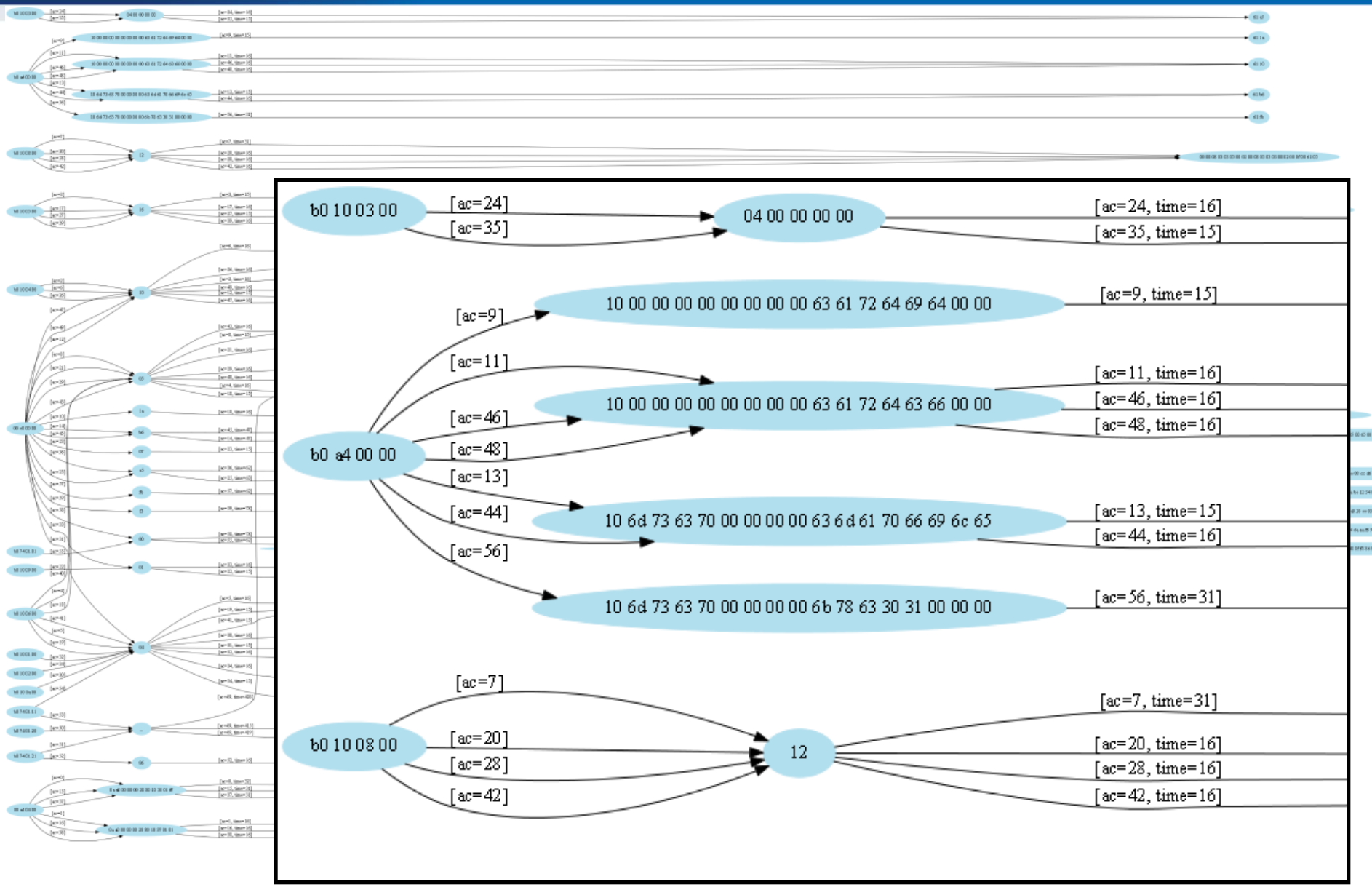
winscard.dll

```
[begin]
SCardTransmit (handle 0xEA010001)# apduCounter:0#
totalBytesINCounter:1#
transmitted:00 a4 04 00 0a a0 00 00 00 28 80 10 30 01 ff
responseTime:31#
SCardTransmit result:0x0#
received:6a 81

SCardTransmit (handle 0xEA010001)# apduCounter:1#
totalBytesINCounter:16#
…
```






b0 10 03 00
[ac=24]
[ac=35]
04 00 00 00 00
[ac=24, time=16]
[ac=35, time=15]
10 00 00 00 00 00 00 00 00 63 61 72 64 69 64 00 00
[ac=9]
[ac=9, time=15]
[ac=11]
[ac=11, time=16]
10 00 00 00 00 00 00 00 00 63 61 72 64 63 66 00 00
[ac=46]
[ac=46, time=16]
[ac=48]
[ac=48, time=16]
b0 a4 00 00
[ac=13]
[ac=13, time=15]
[ac=44]
10 6d 73 63 70 00 00 00 00 63 6d 61 70 66 69 6c 65
[ac=44, time=16]
[ac=56]
10 6d 73 63 70 00 00 00 00 6b 78 63 30 31 00 00 00
[ac=56, time=31]
[ac=7]
[ac=7, time=31]
b0 10 08 00
[ac=20]
12
[ac=20, time=16]
[ac=28]
[ac=28, time=16]
[ac=42]
[ac=42, time=16]

Open topics

- More functionality into APDUPlay, better representation of results
- …

ANTLR v3

http://cesta.sourceforge.net

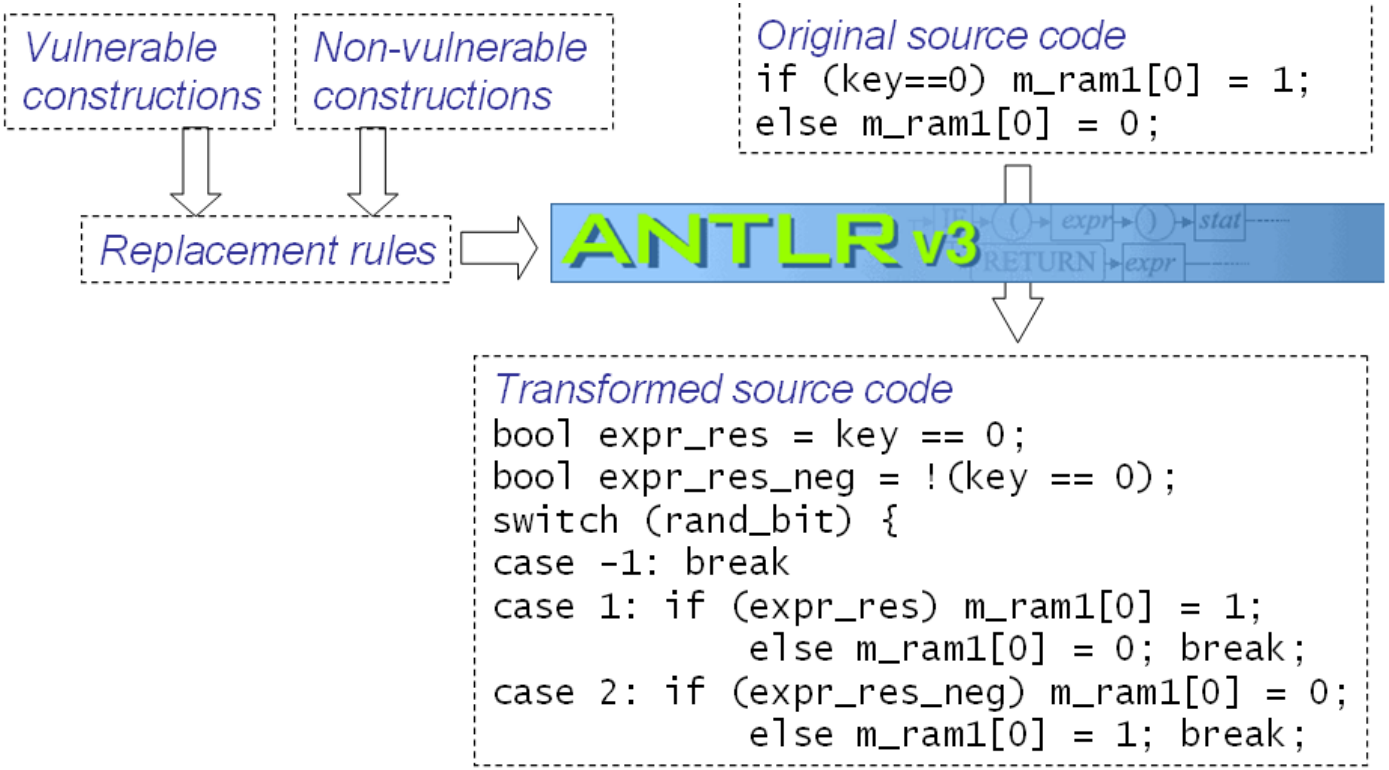
AUTOMATED SOURCE CODE TRANSFORMATION

CesTa - main design goals

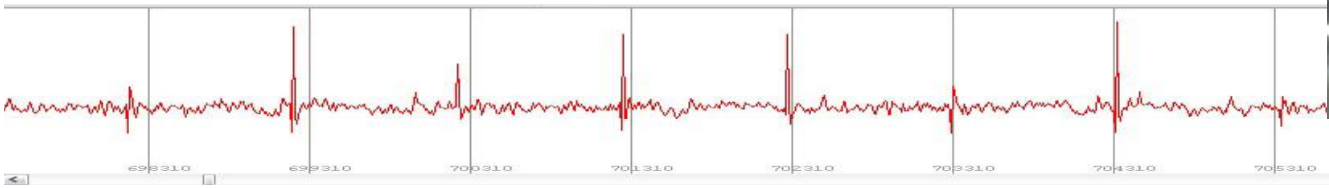
1. Enhanced security on real applets
   - fix what is wrong, add preventive defenses
2. Source code level & auditability
   - trust, but verify
3. Complexity is hidden
   - clarity of original code
4. Flexibility & Extensibility
   - protect against new threats
   - protect only what HW does not

CesTa – basic scheme

- Write code once, apply only what needed



Another attack – fault induction



- Attacker can induce bit faults in memory locations
  - power glitch, flash light, radiation...
  - harder to induce targeted then random fault

01011010

10100101

- Protection with shadow variable
  - every variable has *shadow* counterpart
  - shadow variable contains *inverse* value
  - consistency is checked every read/write to memory

a **01011010**

a_inv 10100101

if (a != ~a_inv) Excepti
a = 0x55;
a_inv = ~0x55;

01010000

10101010

if (a != ~a_inv) Exception();
a = 0x13;

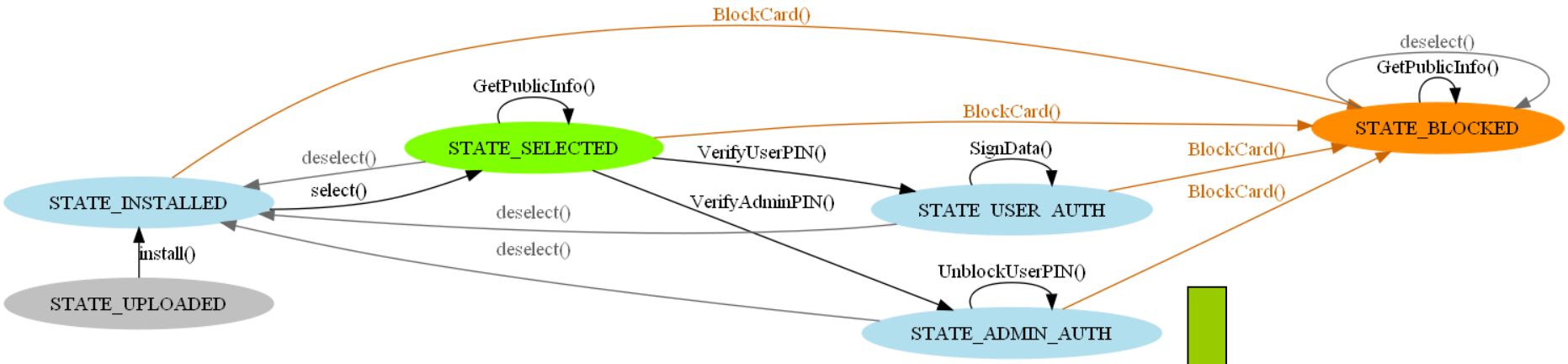
- Robust protection, but cumbersome for developer

Applet state transition enforcement

- Applet security states controlled usually ad-hoc
  - *if (adminPIN.isValidated() && bSecureChannelExists)* …
  - unwanted (unprotected) paths may exist
- Possible solution
  - model state transitions in inspectable format (DOT (GraphViz)
  - automatical
  - check appro

```
digraph StateModel {
rankdir=LR;
size="6,6";
node [shape =ellipse color=lightblue2, style=filled];

{ rank=same; "STATE_UPLOADED";"STATE_INSTALLED";}
"STATE_INSTALLED" [color=lightblue2, style=filled];
"STATE_UPLOADED" [color=gray, style=filled];
"STATE_UPLOADED" -> "STATE_INSTALLED" [label="install()"];
```




```
private void SetStateTransition(short newState) throws Exception {
  // CHECK IF TRANSITION IS ALLOWED
  switch (m_currentState) {
    case STATE_UPLOADED: {
        if (newState == STATE_INSTALLED) {m_currentState = STATE_INSTALLED; break;}
        throw new Exception();
    }
    case STATE_INSTALLED: {
        if (newState == STATE_SELECTED) {m_currentState = STATE_SELECTED; break;}
        if (newState == STATE_BLOCKED) {m_currentState = STATE_BLOCKED; break;}
        throw new Exception();
    }

    case STATE_SELECTED: {
        if (newState == STATE_SELECTED) {m_currentState = STATE_SELECTED; break;}
        if (newState == STATE_USER_AUTH) {m_currentState = STATE_USER_AUTH; break;}
        if (newState == STATE_ADMIN_AUTH) {m_currentState = STATE_ADMIN_AUTH; break;}
        if (newState == STATE_BLOCKED) {m_currentState = STATE_BLOCKED; break;}
        if (newState == STATE_INSTALLED) {m_currentState = STATE_INSTALLED; break;}
```

Thank you for your attention!

Questions