Smart cards en EMV

Joeri de Ruiter

Digital Security, Radboud University Nijmegen

Smart cards

- Processor en geheugen
- Contact of draadloos
- Tamper resistant
- Gebruikt voor
  - Bankpassen
  - OV Chipkaart
  - SIM kaarten
  - Paspoort

Smart cards

- Cryptografische co-processor
- Pseudo random number generator
- Meerdere applicaties mogelijk
- Programmeertalen
  - C (MULTOS)
  - Java (JCOP)
  - Basic (BasicCard)

Smart cards

- ISO 7816
  - Van fysieke specificaties tot commando's
- Master-slave
- Application Protocol Data Units (APDUs)
  - Commands

CLA	INS	P1	P2	Lc	Data	Le

  - Responses

Data	SW1	SW2

Smart cards

- VERIFY
  - > 00 20 00 80 08 24 12 34 FF FF FF FF FF
    - 00 20 – VERIFY
    - 00 80 – Plaintext PIN
    - 08 – Lengte data
    - 24 12 34 FF FF FF FF FF – Data
  - < 90 00
    - PIN code correct

Wat is EMV?

Standaard voor betalingen met smart cards

Wat is EMV?

Ontwikkeld en onderhouden door

Eigendom van

Wat is EMV?

- Ontwikkeling begonnen in 1993
- Wereldwijd meer dan 1,5 miljard kaarten
- Sinds begin 2012 overal in gebruik in Nederland
- Standaard meer dan 700 pagina's
- Varianten voor draadloze en internet betalingen

Waarom EMV?

- Tegengaan fraude
  - Skimmen
  - Card-not-present fraude

- Internationale afspraken

Set-up sleutels

- Kaart en bank: symmetrische sleutel (3DES)
  - Authenticiteit transacties
- Bank: private/public keypair (RSA)
  - Authenticiteit kaarten
- Kaart (optioneel): private/public keypair (RSA)
  - Authenticiteit transacties en kaarten

EMV sessie

- Initialisatie
  - Selecteren applicatie
  - Uitlezen data
- Kaart authenticatie
- Kaarthouder verificatie
- Transactie

Kaart authenticatie

- Static Data Authentication (SDA)
  - Statische data getekend door issuer

READ RECORD

Sig((rek.nr., pas nr., …), skBank)

Kaart authenticatie

- Dynamic Data Authentication (DDA)
  - Gebruik van asymmetrische crypto
  - Challenge/response mechanisme

READ RECORD →

← Sig((rek.nr., …,pkKaart), skBank)

INTERNAL AUTH, nonceT →

← Sig((nonceT, nonceK), skKaart)

Kaart authenticatie

- Combined Data Authentication (CDA)
  - Transactie data getekend

READ RECORD

Sig((rek.nr., …,pkKaart), skBank)

GENERATE AC, bedrag, nonceT, ...

Sig((bedrag, nonceT, …, AC), skKaart)

Kaarthouder verificatie

- Geen
- Handtekening
- PIN code
  - Offline
    - Wel of geen encryptie
  - Online

Transactie

- Application Cryptograms
  - Transaction Certificate (TC)
  - Application Authentication Cryptogram (AAC)
  - Authorisation Request Cryptogram (ARQC)
- MAC over transactie data
- Online
  - Authenticatie bank
- Offline
  - Geen contact bank

EMV-CAP

- Standaard voor internetbankieren
- Niet openbaar maar grotendeels achterhaald
- In gebruik bij
  - Rabobank (Random Reader)
  - ABN AMRO (e.dentifier)

EMV-CAP

PIN

challenge

bitfilter(AC)

PIN

OK

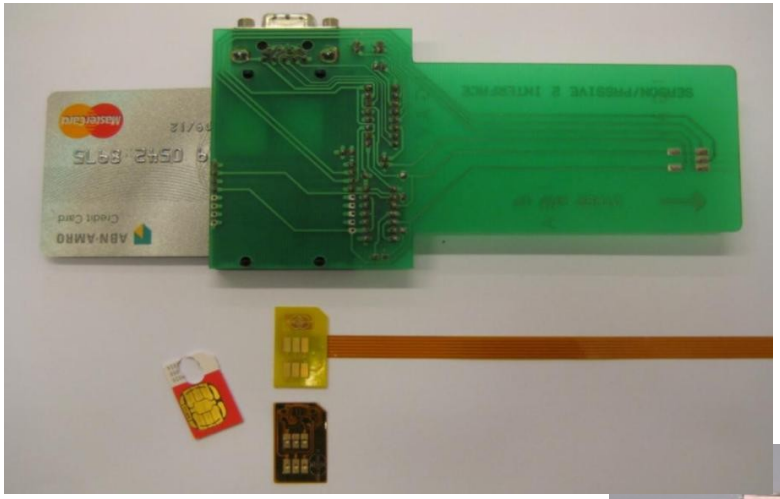
GENERATE AC (challenge,...)

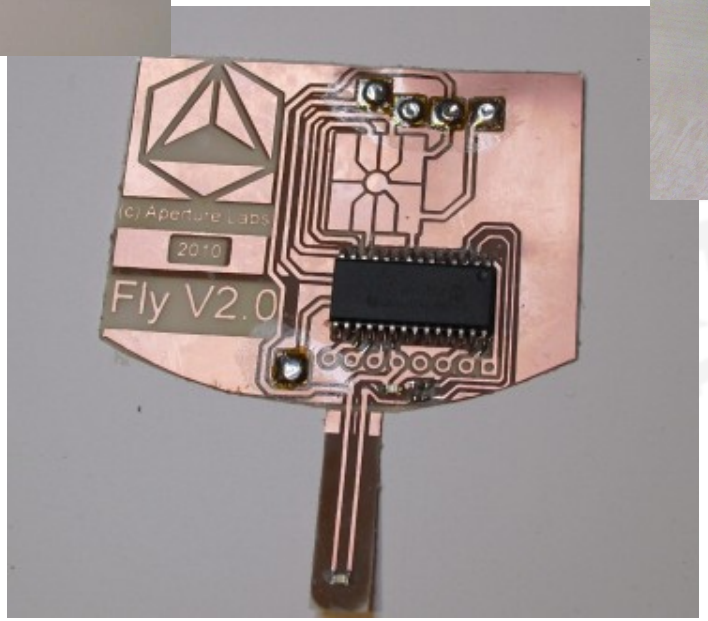
AC

Aanvallen op smart cards

- Direct uitlezen geheugen niet mogelijk
- Passief
  - Afluisteren communicatie
- Actief
  - Man-in-the-middle aanval
  - Aanpassen communicatie
- Side channels
  - Stroomverbruik
  - Elektromagnetische straling

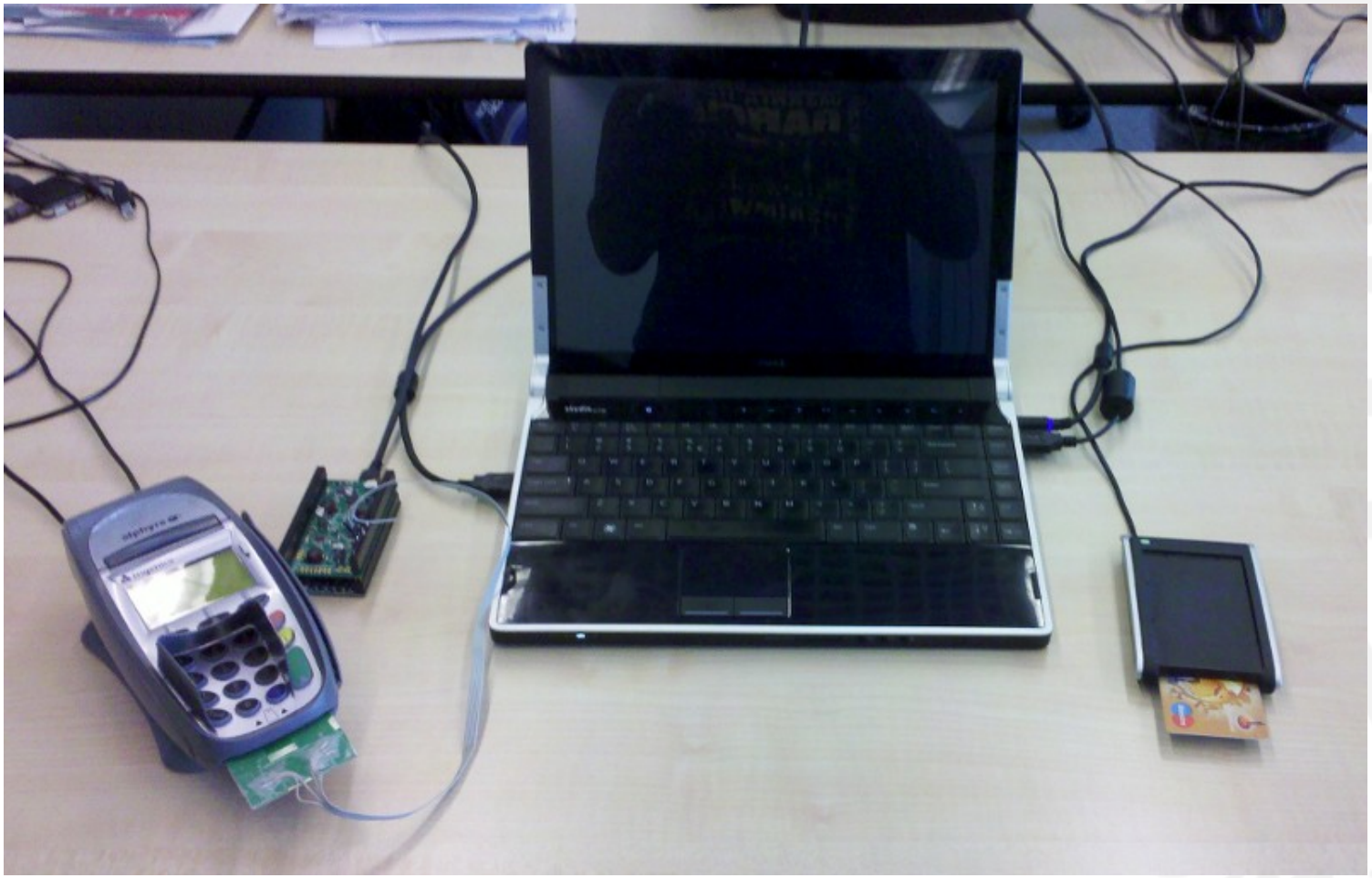
Aanvallen op smart cards





SmartLogic

- Ontwikkeld door Gerhard de Koning Gans



Bekende zwakheden

- Skimmen
  - Benodigde data voor magneetstrip op de chip
  - e.dentifiers ABN AMRO vervangen in filialen
    - 2008, 2009
    - 1,5 miljoen euro schade
    - Downloadpas

Bekende zwakheden

- Klonen SDA kaarten
  - Mogelijk voor offline transacties
  - Alleen statische data geauthenticeerd
  - Kaart ondersteunt geen asymmetrische crypto
  - Yes-card
    - Alle PIN codes geaccepteerd

Bekende zwakheden

- DDA man-in-the-middle aanval
  - Mogelijk voor offline transacties
  - Terminal kan transactie niet authenticeren
  - Transactie niet verbonden met authenticatie kaart

INTERNAL AUTH, nonceT

Sig((nonceT, nonceK), skKaart)

GENERATE AC

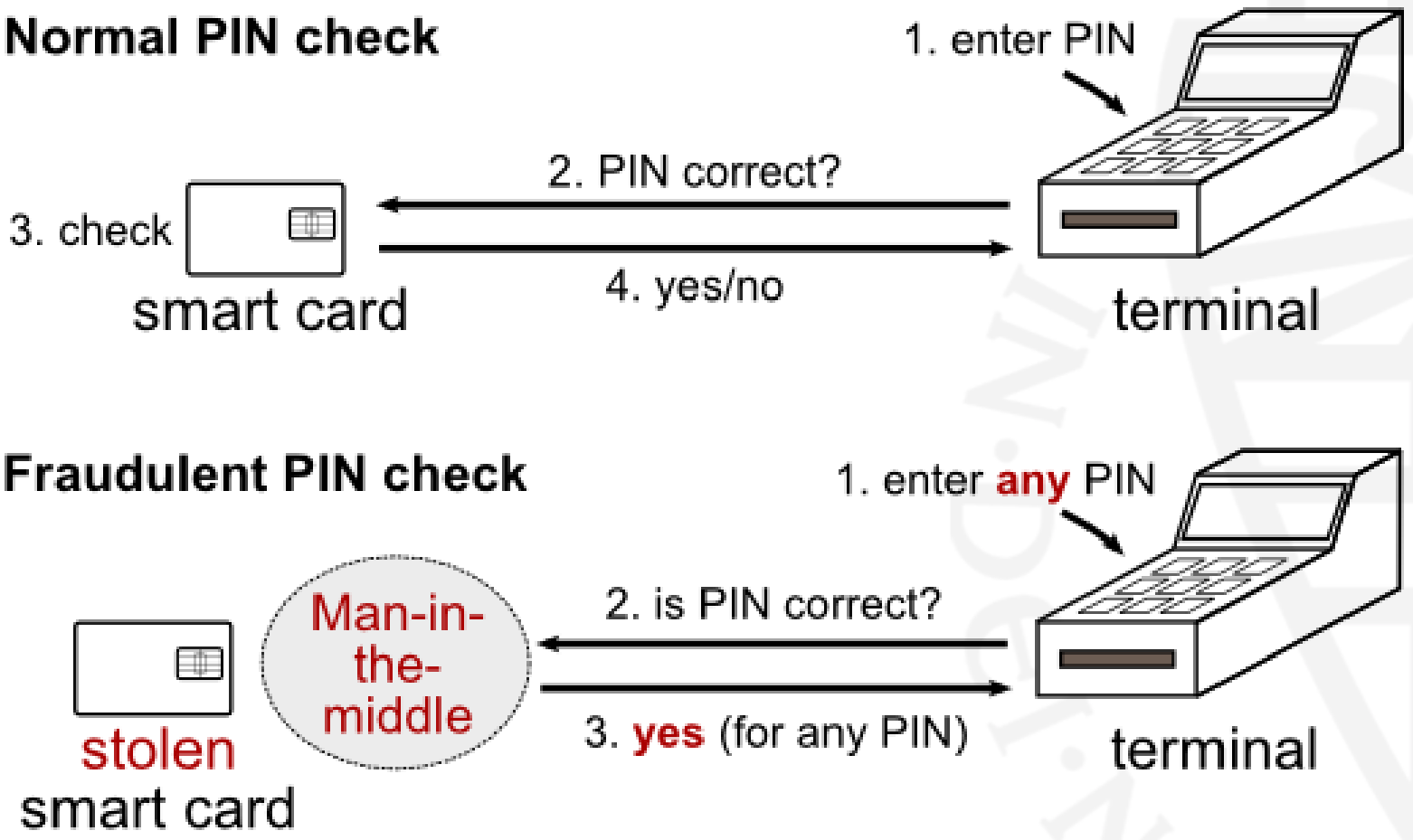
AC

MitM

Bekende zwakheden

- “Chip & PIN is broken” [Murdoch et al. 2010]
  - Mogelijk voor offline en online transacties
    - Als de kaart niet geblokkeerd is
    - Als transacties zonder PIN zijn toegestaan
  - Man-in-the-middle aanval
  - Alle PIN code geaccepteerd
  - Niet mogelijk in Nederland

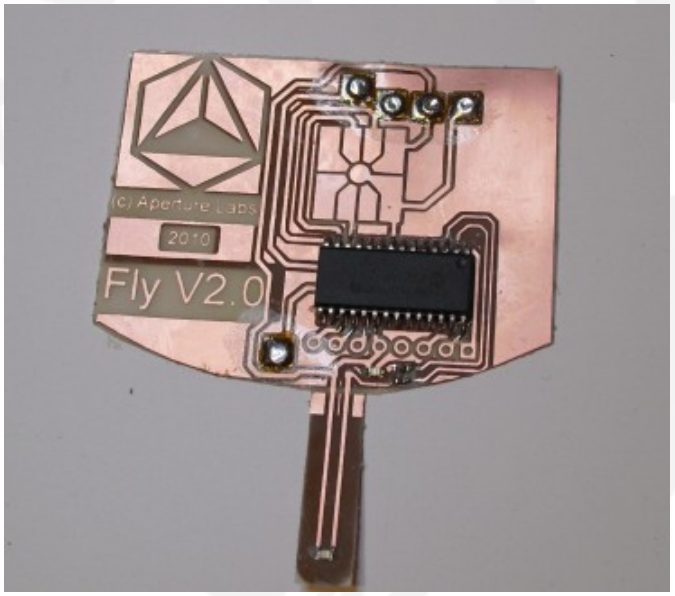
Bekende zwakheden



Bron: https://www.cl.cam.ac.uk/research/security/banking/nopin/

Bekende zwakheden

- “Chip & PIN is definitely broken” [Barisani et al. 2011]
  - Rollback naar plaintext PIN
  - Terminals in Nederland gepatcht
  - Aanval mogelijk
    - Gedetecteerd in backend



Bekende zwakheden

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	