Digitaal betalen & bankieren

Erik Poll

Digital Security

Radboud University, Nijmegen, the Netherlands

Banken & cyber security

Banks a long-time favourite target of criminals

Also of *cyber* criminals

This produces lots of anecdotes, but also historical trends, that we can learn from

Biggest cyber bank robbery to date

$ 951 million stolen via SWIFT global payment system from the Bangladesh Central Bank

- **Most of the money recuperated ;**
  'Only' $ 81 million really lost, via casinos on the Philippines
- **Attackers installed custom malware on computers at bank & clearly had insider knowledge**
  - **Malware removed transactions from local database & physical print-outs, to delay detection**

These are no script kiddies, but serious organised crime or state actors

[http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html]

[http://www.reuters.com/assets/iframe/cmsyovideo?videoId=370707923]

[https://www.nettitude.com/wp-content/uploads/2016/12/Nettitude-SWIFT-Threat-Advisory-Report-client.pdf]

Topics

1. Pinnen & chippen
2. Online payments & internet banking
3. Contactless payments
4. Side-channel attacks

5. Some general observations on cyber security

Skimming

Skimming

Magnetic-stripe (mag-stripe) on bank card contains digitally signed information

but… this info can be copied

Do you see anything suspicious?

Skimming

Camera to see
PIN being entered

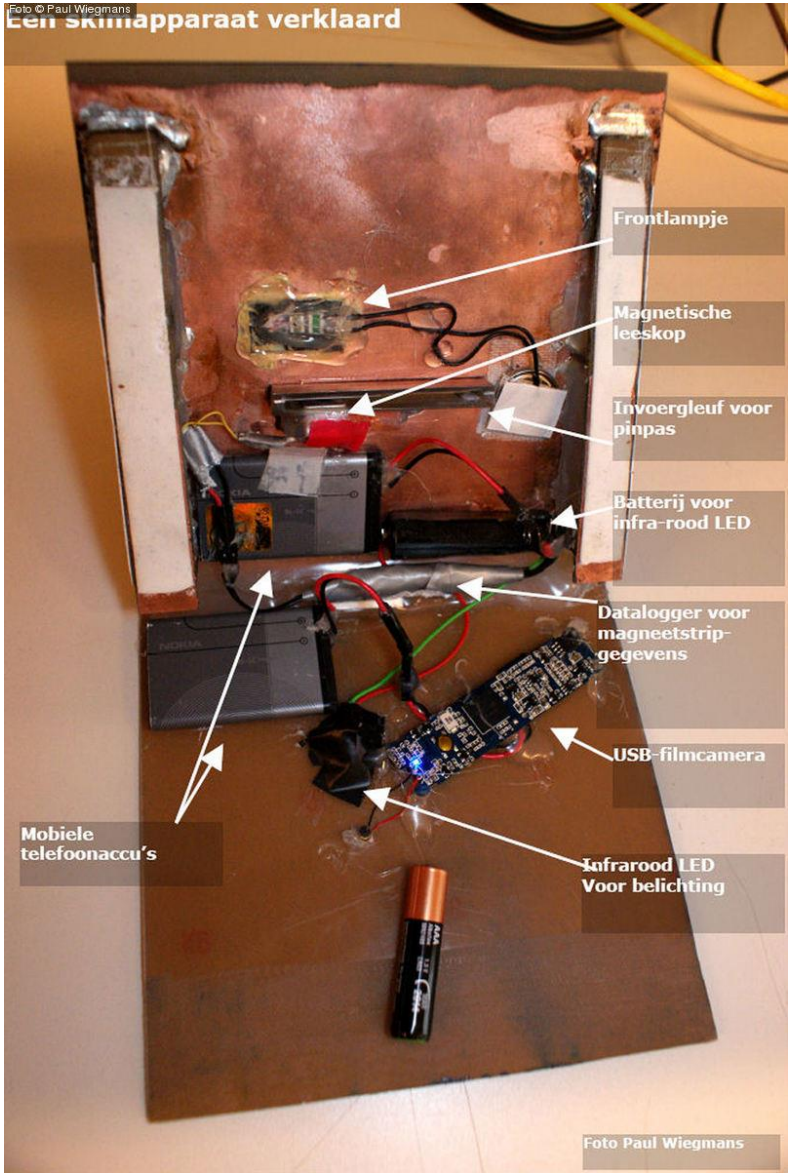
Fake cover
that makes
copy of the
magnetic stripe

More skimming equipment

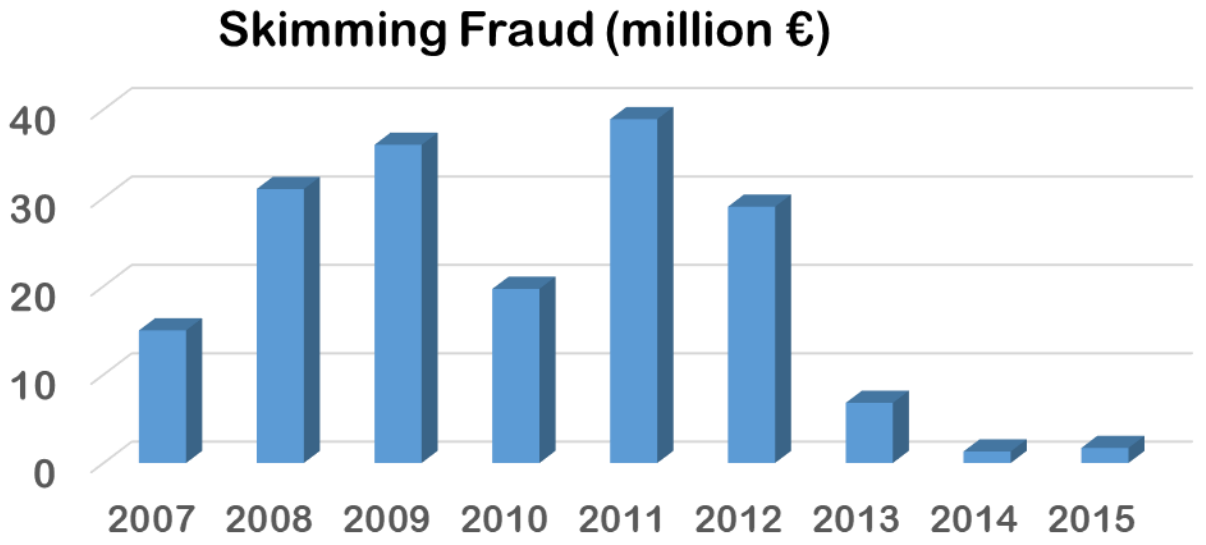
Fake keyboard
to intercept PIN code

Fake cover
that copies magnetic stripe

Skimming apparatuur



Skimming fraud in the Netherlands



[Source: NVB & Betaalvereniging]

Fraud under control thanks to

- better monitoring & response (incl. blocking cards)
- replacing of mag-stripe by chip  in 2012

EMV (Europay-Mastercard-Visa)

- Standard used by all chip cards for banking
- Specs controlled by EMVCo which is owned by

- Unlike magstripe, a smartcard cannot be cloned, because it uses a challenge-response protocol

challenge **c**

c encrypted with **K**

- Payment terminal sends a *different* challenge c every time, so card gives a *different* response each time
- Card proves it knows the secret key K without revealing it
- This can use symmetric crypto or asymmetric crypto (aka public key crypto). In the latter case, the secret key will be a private key.

Challenge-response systemen kraken

http://www.cs.ru.nl/chares

Twee vragen

1) Kun je door verschillende sleutels & challenges te proberen *achterhalen hoe de versleuteling werkt?* (reverse engineering)

2) Als je weet hoe de versleuteling f werkt: kun je door verschillende challenges te proberen *achterhalen wat de sleutel is?* (cryptanalysis)

Voor goede versleutelingsalgoritmes, zoals in bankpassen gebruikt worden, is 2) niet te doen, maar bij de ov-chipkaart (Mifare Classic) kan het wel.

Does EMV chip  reduce skimming?

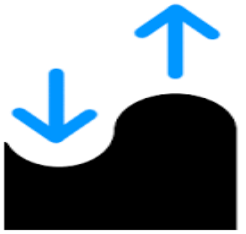
- UK introduced EMV in 2006

	2005	2006	2007	2008
domestic	79	46	31	36
foreign	18	53	113	134

Skimming fraud with UK cards, in millions £

- Copied magstripes can still be used in countries that don't use the chip
- Blocking cards for use outside EU (geoblocking) helps a lot!
- Skimmers have now moved to the US, and the US is now migrating to EMV

Such water bed effects are a recurring phenomenon



Recurring problem: BACKWARD COMPATIBILITY

- In 2009, criminals put tampered card readers *inside* Dutch bank branches to skim cards
  - For *backwards compatibility*, the chip reports the mag-stripe data...
  - Both mag-stripe data and PIN code sent *unencrypted* from card to this reader
  - Criminals caught & convicted in 2011

- Cards have been improved to avoid this:
  mag-stripe data should now be different from info on the chip

More low-tech attacks: PHISHING

Criminals have sent emails asking people to return their bank card & pin code by post to the bank

Rabobank waarschuwt voor nieuwe phishing: stuur nooit je pas op

De Rabobank waarschuwt voor een nieuwe vorm van phishing, waarbij het slachtoffer wordt gevraagd om een zogenaamd verlopen betaalpas op te sturen.

Oplichters 'hengelen' opnieuw naar bankpassen

Alert 17-10-2017 3 reacties

Moral of the story:

- **Some people are really easy to fool**
- **Attackers are very creative in coming up with new attacks**

From: Rabobank
Sent: Sunday, June 26, 2016 10:21 PM
To: [redacted]
Subject: De nieuwste wijziging van onze producten

Rabobank

Geachte klant,

Als klant van de Rabobank, blijft u graag op de hoogte van nieuwe veranderingen op het gebied van betaalproducten.

De Rabobank introduceert nu de nieuwe NFC-2 betaalpas.
De NFC-2 volgt de eerdere versie op. Met de NFC-2 betaalpas bent u beter beschermd tegen pinpasfraude. De nieuwe betaalpas maakt gebruik van de nieuwste beveiliging. De nieuwe betaalpas is niet alleen gemakkelijker, maar ook veiliger. Alle betaalpassen dienen daarom vervangen te worden. De Rabobank denkt veel aan de toekomst en wilt de vervanging van alle betaalpassen zo milieuvriendelijk laten verlopen. Daarom recyclen we alle huidige passen, de nieuwste technologie maakt het mogelijk om de chip op de passen te vervangen.

Recycle procedure
Wij vragen onze klanten zich aan te melden voor de recycle procedure. Door u aan te melden voor de recycle programma

Problem: COMPLEXITY

EMV is not a protocol, but a 'protocol toolkit suite' with *lots* of configuration options

- **Original EMV specs : 4 books, > 700 pages**
  - **3 types of cards (SDA,DDA, CDA), 5 authentication mechanism (online PIN, online PIN, offline encrypted PIN, signature, none), 2 types of transactions (offline, online), ….**

Sample sentence

"If the card responds to GPO with SW1 SW2 = x9000 and AIP byte 2 bit 8 set to 0, and if the reader supports qVSDC and contactless VSDC, then if the Application Cryptogram (Tag '9F26') is present in the GPO response, then the reader shall process the transaction as qVSDC, and if Tag '9F26' is not present, then the reader shall process the transaction as VSDC."

Offline vs Online PIN

- An EMV transaction can be without PIN
  - Eg: credit card payment for motorway in France; contactless payments
- If an EMV transaction is with PIN, then there are two possibilities
  1. Online PIN: PIN is sent to the bank for verification
     - This is what most Dutch ATMs & payment terminals do
  2. Offline PIN: PIN is sent to the chip for verification
     - This has to be used if payment terminal is offline, and in internet banking tokens

     Two variants of offline PIN

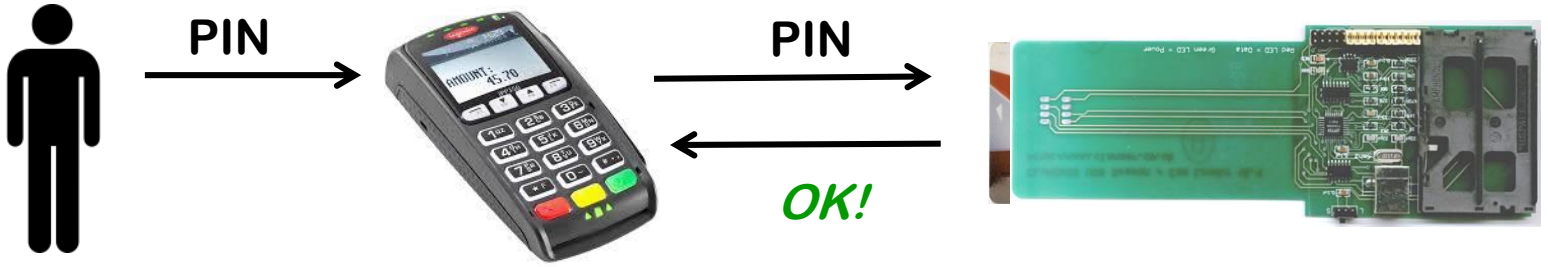
     2a) PIN is sent plaintext to the chip

     2b) PIN is sent over encrypted channel between chip & terminal

Complexity: example protocol flaw

Terminal can choose to do offline PIN

- ie. terminal asks the card to check the PIN code



The OK response of the card is *not authenticated*

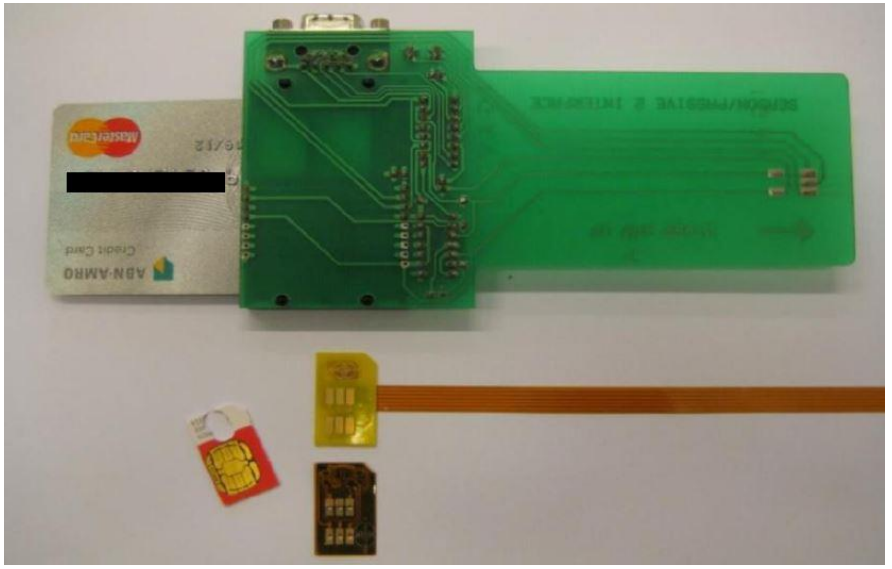
- ie. not cryptographically signed

so offline terminal can be fooled by a Man-in-the-Middle attack

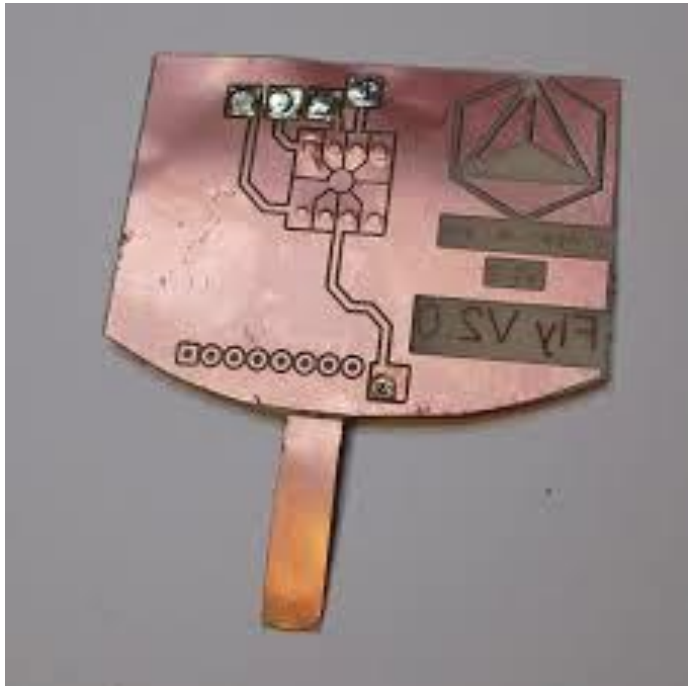
The transaction data will reveal the transaction was PIN-less, so the bank back-end will know the PIN was *not* entered

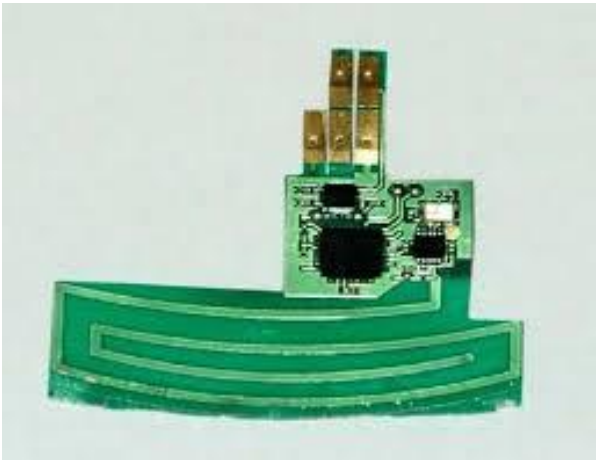
[Stephen Murdoch et al., *Chip & PIN is broken*, FC'2010]

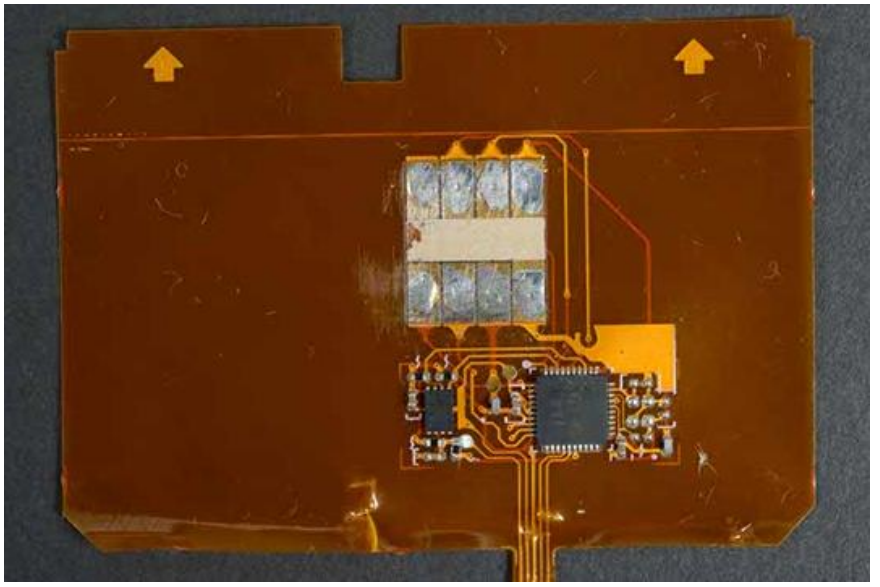
Our Man-in-the-Middle set-up



More fancy & criminal MitM equipement



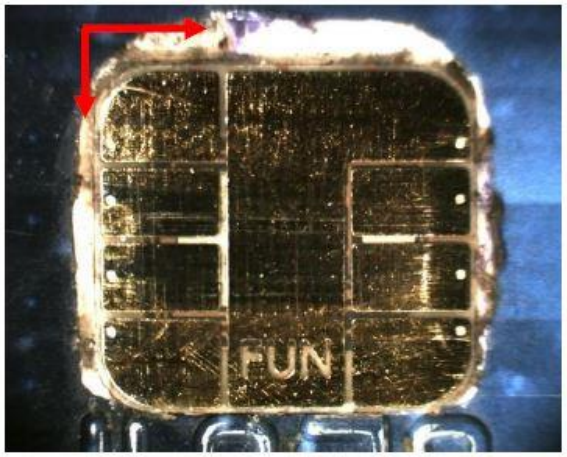


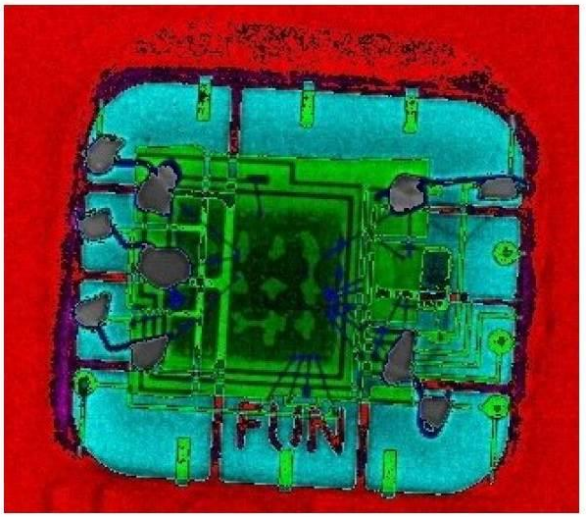


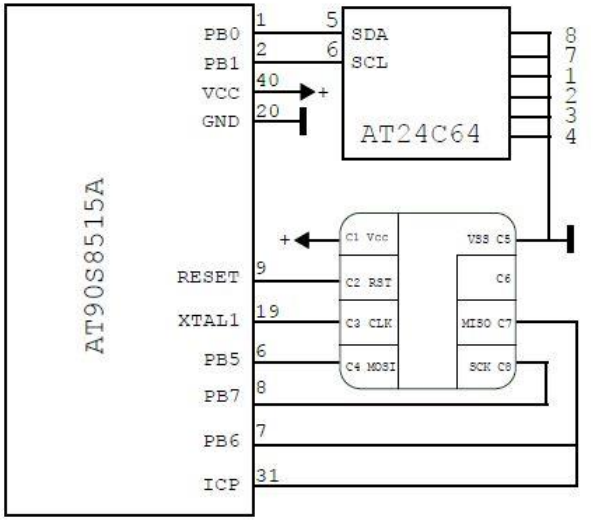
https://krebsonsecurity.com/tag/atm-shimming/

Criminal Man-in-the-Middle set-up

Chips from stolen cards inserted under another chip, which faked the PIN OK response



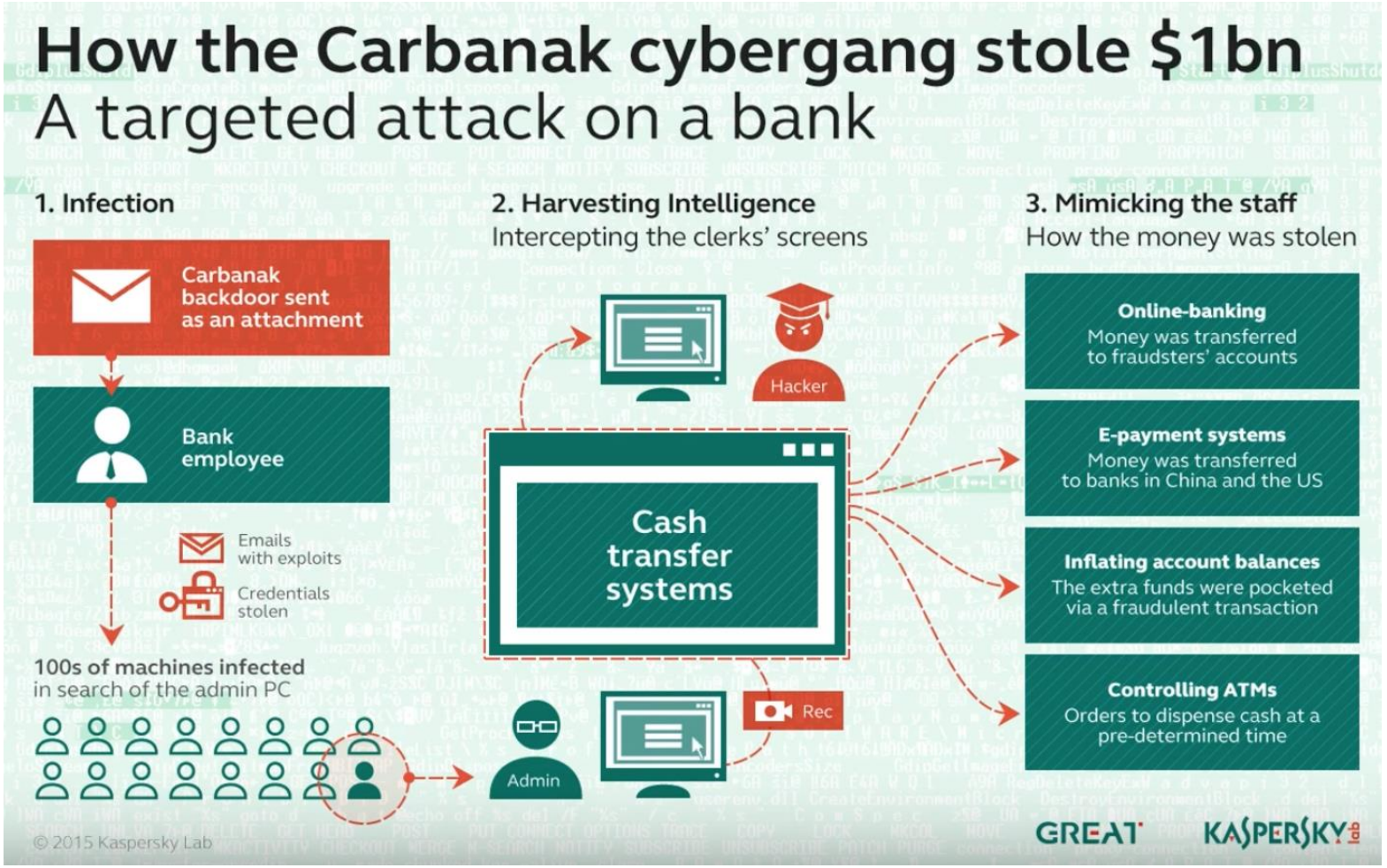




xray reveals green stolen chip under blue microcontroller

[Houda Ferradi et al., *When Organized Crime Applies Academic Results: A Forensic Analysis of an In-Card Listening Device*, Journal of Cryptographic Engineering, 2015]

ATM hacking



Darknet Diaries podcast **https://darknetdiaries.com/episode/35**

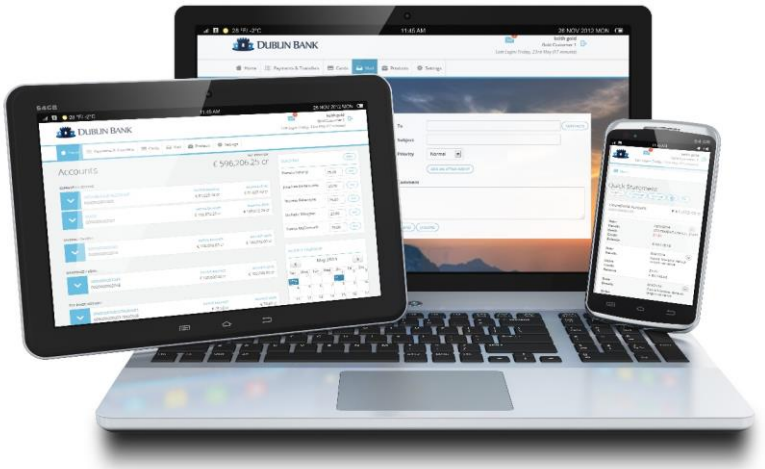
- Darknet Diaries is een Amerikaanse podcast heeft meer leuke verhalen over cyber security

- Bijv
  - aflevering over DigiNotar

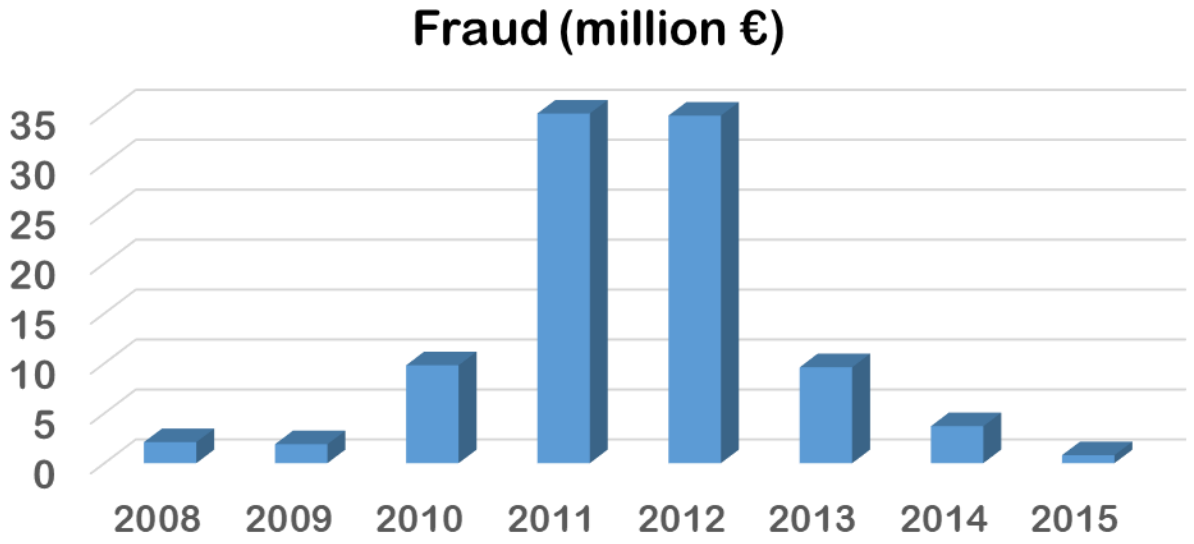
    https://darknetdiaries.com/episode/3/
- aflevering over StuxNet

  https://darknetdiaries.com/episode/29/

Internet banking



Fraud with internet banking in NL



[Source: NVB & Betaalvereniging]

Fraud under control thanks to:

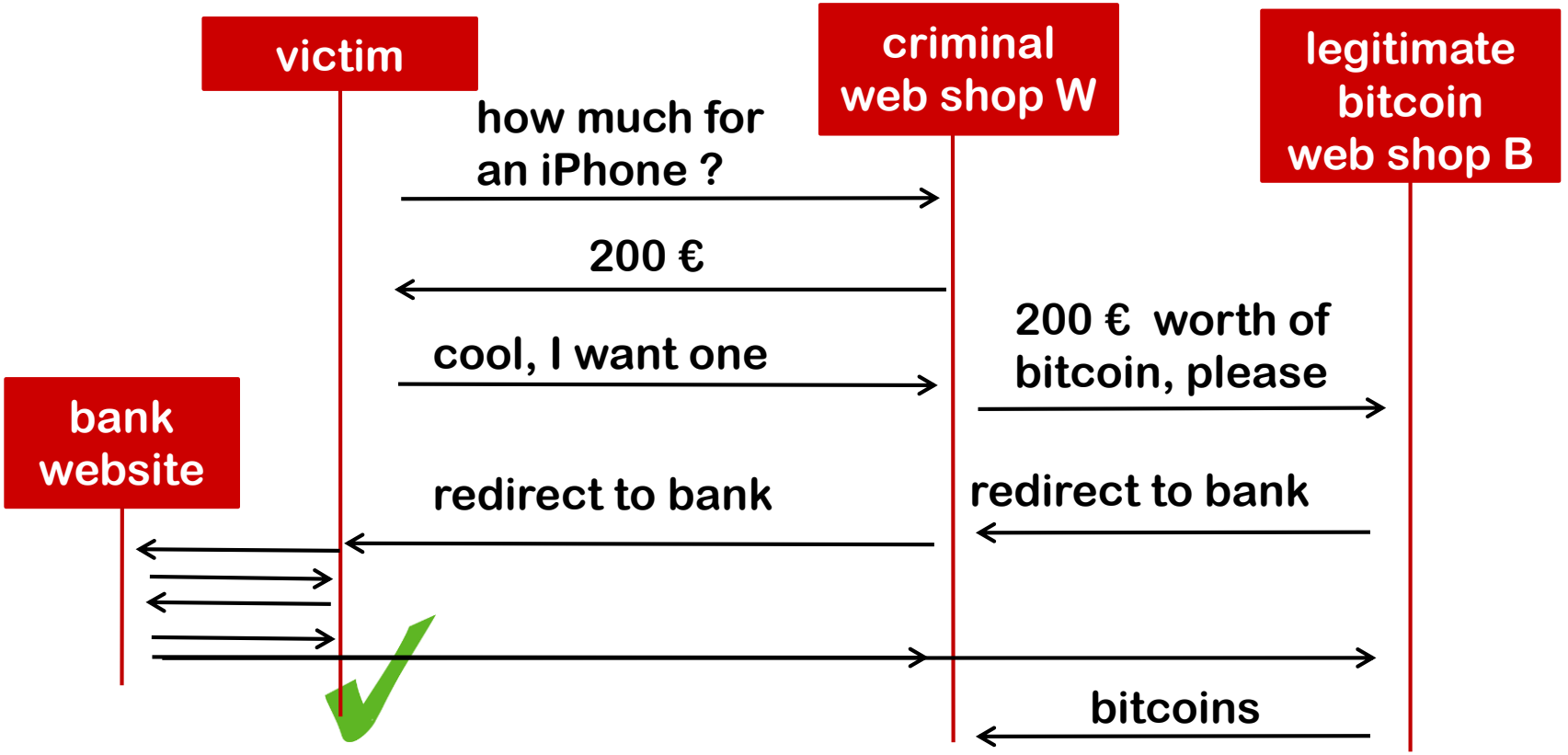
1. better monitoring - for suspicious transactions & money mules
   - finding money mules, to extract money from the system without being caught, is a bottleneck for attackers
2. awareness campaigns
3. criminal switching to ransomware as better business model?

Example attack on internet banking (1)

- Your online bank statement shows you received 3000 euro from some company you never heard of
- You get a phone call or email from the bank, saying that this is a mistake and asking you to transfer the money back

- You never received 3000 euro, but malware in your browser inserts the fake transaction
  - this is a so-called Man-in-the-Browser attack
- When you transfer the money back, that is not a fake transaction…

Example attack on internet banking (2)



- Problem: messages to users not very informative, so they don't spot that they are buying bitcoins from B, not an iPhone from W
- Solution: better monitoring, and banks impose extra rules on bitcoin shops & online casinos for allowing internet payments

Contactless payments

Contactless payments

Contactless version of EMV with bank card or NFC smartphone

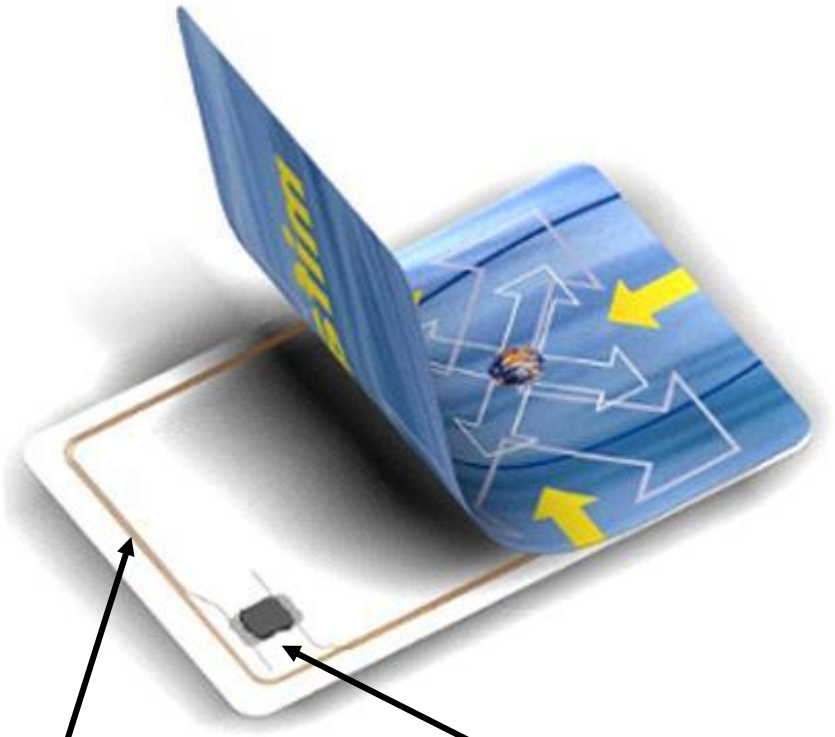
- NFC technology in phones is compatible with the particular form of RFID technology used in contactless bank cad

In Netherlands, for a maximum of 25 euro per individual transaction and a cumulative total of 50 euro until you use your PIN again.

Contactless & dual contact cards

Chip inside bank card can communicate via metal contacts 

or wirelessly via antenna)))



Zelf met contactloze kaarten spelen

- Met een NFC telefoon kun je zelf met contactloze kaarten praten
  - De RFID standaard ISO 14443 is compatible met NFC
- Met de READID NFC passport reader app kun je rijbewijs, ID kaart en paspoort uitlezen
  - Als beveiliging tegen stiekem uitlezen moet je als wachtwoord het pasnummer en verloopdatum opgeven voordat de chip informatie rapporteert. De READ ID app leest deze info met de camera af.
  - Bij automatische paspoortcontrol op bijv. Schiphol moet je paspoort open op het poortje leggen zodat deze info met OCR (Optical Character Recognition) kan worden afgelezen
- Met NXP TagInfo of NFC Taginfo apps kun je basis informatie over een contactloze kaart uitlezen
  - en bijv. zien dat je bankpas en ov-chipkaart een vaste user-ID rapporteert, terwijl het rijbewijs, paspoort en id-kaart hier een willekeurig nummer rapporteert, dat steeds anders is – uit privacy overwegingen

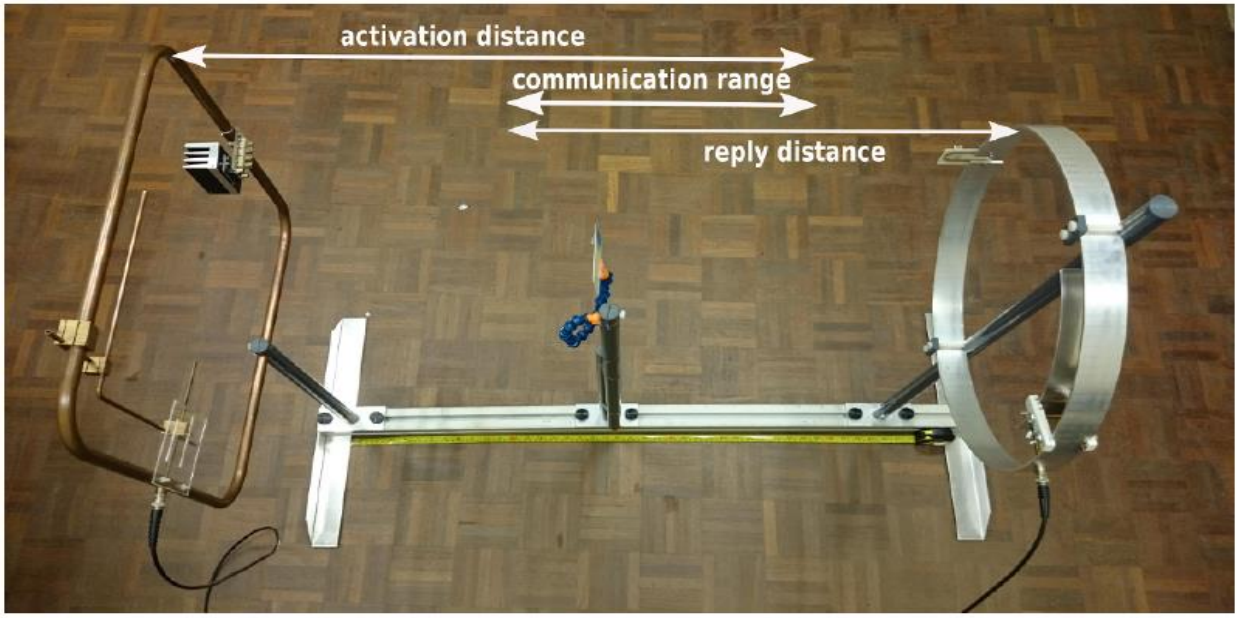
Contactless payments

- ***Who uses a metal container to shield their contactless bank card?***
- ***Who has asked their bank to disable contactless payments for their card?***
- ***Given the choice between a contactless payment without PIN and a contact payment with PIN, which is more secure?***

Attacks on contactless cards

- It is not possible to clone a contactless card
  - because it uses a challenge-response protocol & private key never leaves the chip
- It is possible to do a passive attack
  ie. eavesdrop on wireless communication between terminal & card
  - This is possible at 10-20 meters
- It is possible to do an active attack
  ie. secretly activate card in someone pocket aka digital pickpocketing
  - This is possible at 40-50 cm
    - Activating the card requires a strong magnetic field

Our set-up for active attacks

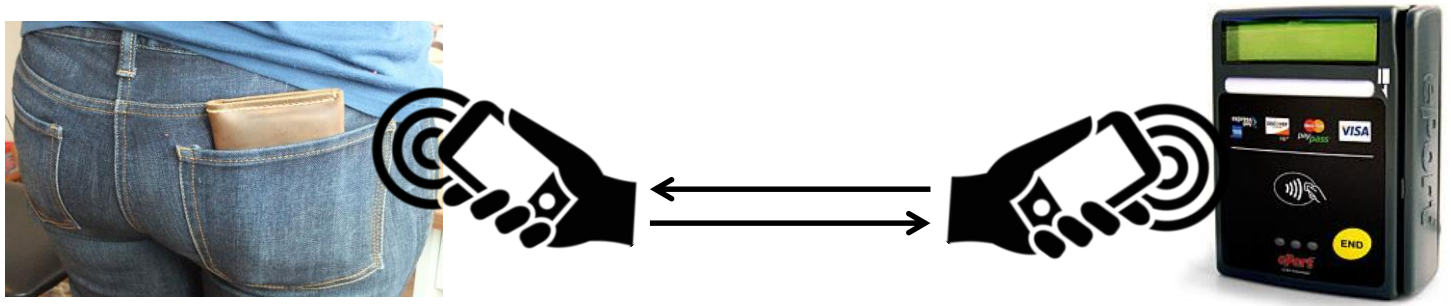


- Max. distance to activate card ≈ 40 cm
- Requires very powerful antenna ≈ 100 Watt

[René Habraken et al., An RFID Skimming Gate Using Higher Harmonics, RFIDSec 2015]

Relay attacks

It is not possible to clone a contactless card,
but it is possible to do a relay attack



- This is an active attack, so requires attacker to get close
- Normally relay attacks are difficult, because of time-outs if relay is too slow; but the banks forgot to specify any time out…
- Is there a good criminal business model? Probably not…

Risk assessment of contact(less) payments

1. Risks of contactless payment *without* PIN
   a) You loose max. € 50 if your card is stolen
   b) You loose max. € 25 euro if you fall victim to a relay attack

   Dutch banks typically cover these losses.
2. Risks of contact payment *with* PIN
   a) You don't loose any money if your card is stolen
   b) You can loose €1000 or more if your card is stolen after attacker snooped your PIN code

   Banks will typically not cover these losses…

Counterintuitively, given the choice to pay with or without PIN, the risk is probably lower without PIN

So the 'extra security' of the PIN probably *in*creases risk for customers.

NB: technical security weakness (no PIN) ≠ risk

where risk = likelihood x impact

Mannen in zwembroek stelen bankpas en pinnen duizenden euro's

TILBURG - Twee dieven zijn afgelopen september wel erg ver gegaan om een bankpas te stelen. Ze volgden een man twee weken lang, tot ze in zwembad Stappegoor in Tilburg hun slag sloegen. Ze stalen de bankpas van de man uit een kluisje en konden duizenden euro's pinnen.

[Bron: omroepbrabant.nl, https://www.youtube.com/watch?v=tpVTdj6xg3c]

Attacking smartcards

Attacking bank cards

Thanks to the challenge response protocol,
the secret key never leaves the card

challenge **c**

c encrypted with **K**

How could we extract the key?

1. **Brute-force**: try all the keys
   - Fundamentally impossible given decent key length
2. **Cryptanalysis**: analyse many challenges & encryptions for patterns to reconstruct key
   - Impossible for good peer-reviewed cryptography (we hope…)
3. **Physically attack or observe the smartcard chip**

Side-channel analysis

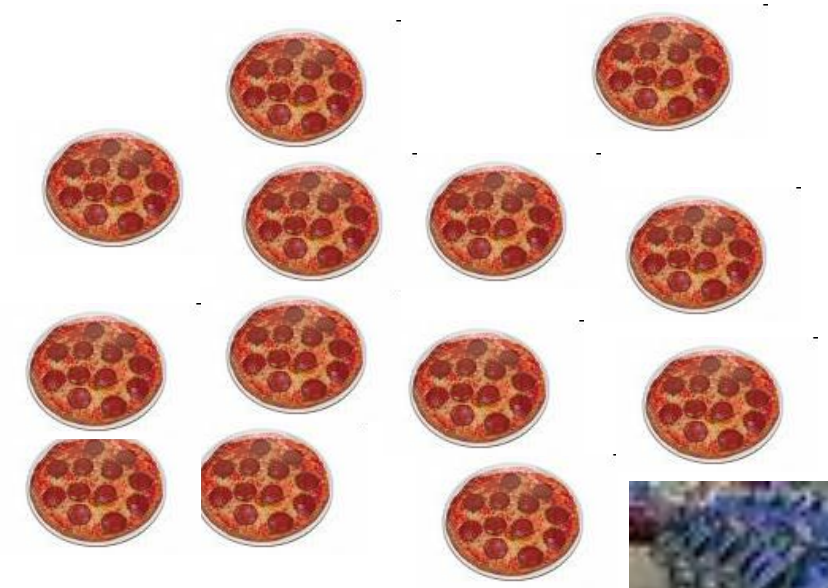
Example side channel:

pizza deliveries to the Pentagon

Side-channel analysis

Thursday evening

Friday evening



On which day will the invasion be?

Side-channel analysis

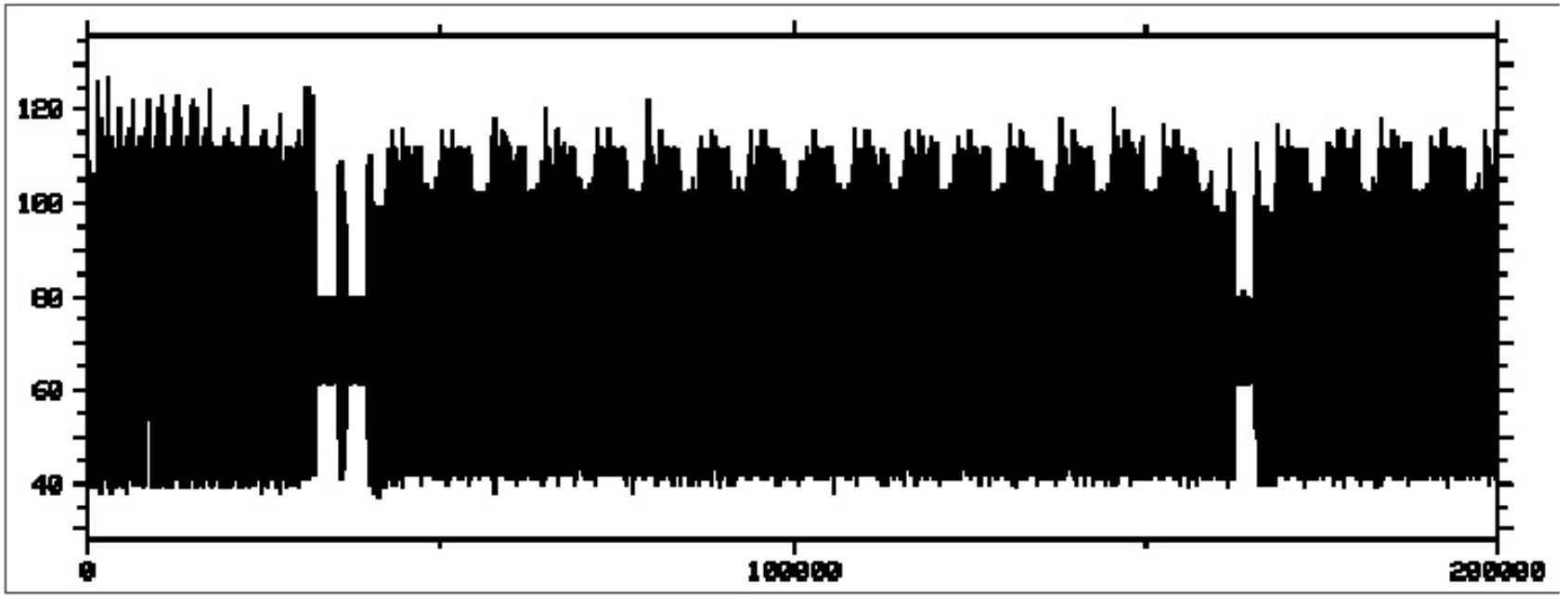
- Side-channel = any other channel than the normal input-output channel that may be observed
- Possible side-channels
  - pizza deliveries
  - sound
  - timing
  - power consumption
  - electro-magnetic radiation

Side channels are very hard to avoid!

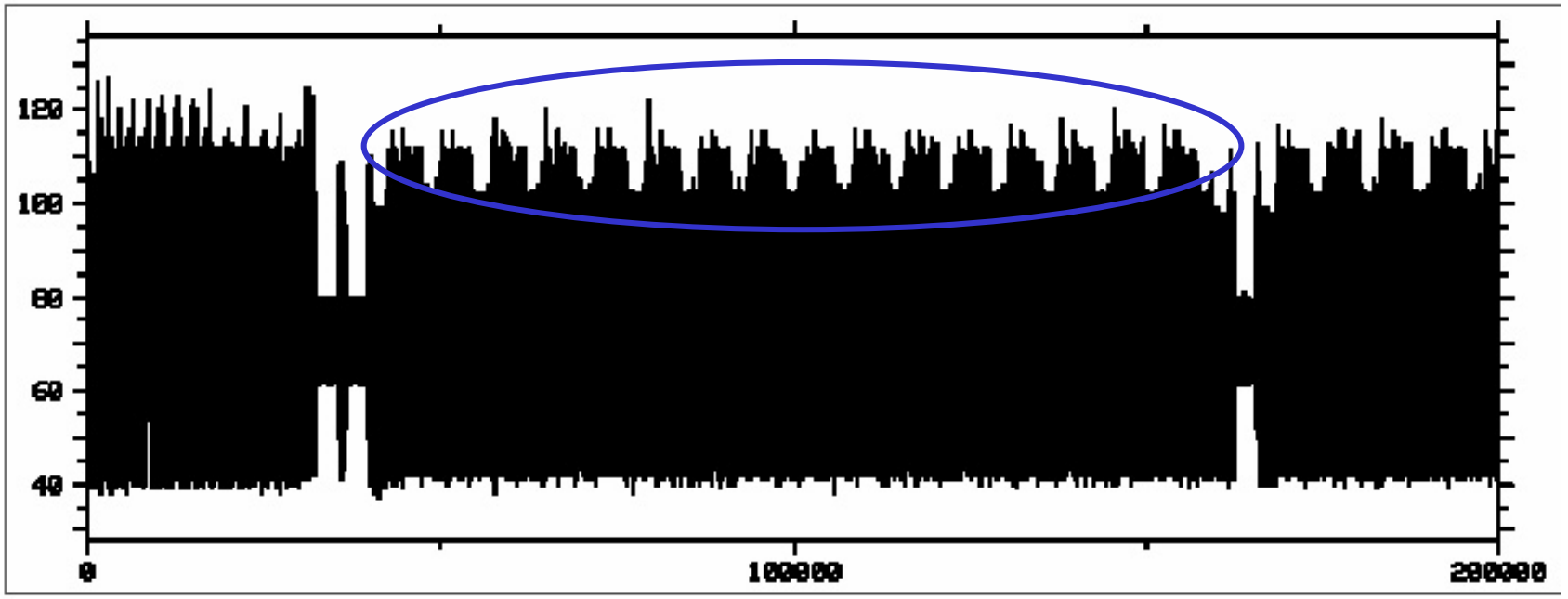
Prof. Lejla Batina in our group does research into side-channels

With Spectre & Meltdown, these attacks are no longer just a concern for smartcards & other cryptographic hardware

Power consumption of a smartcard

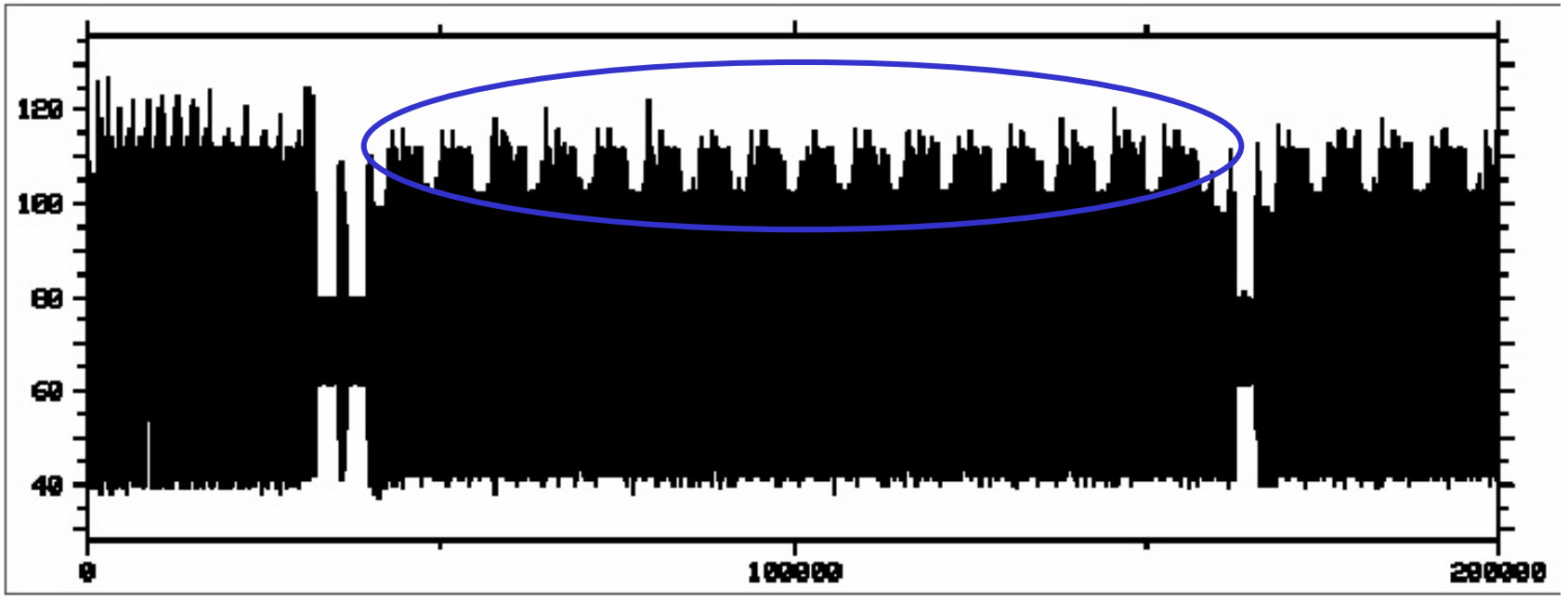


Power consumption of a smartcard



Power consumption of a smartcard

16 rounds, so probably a DES encryption

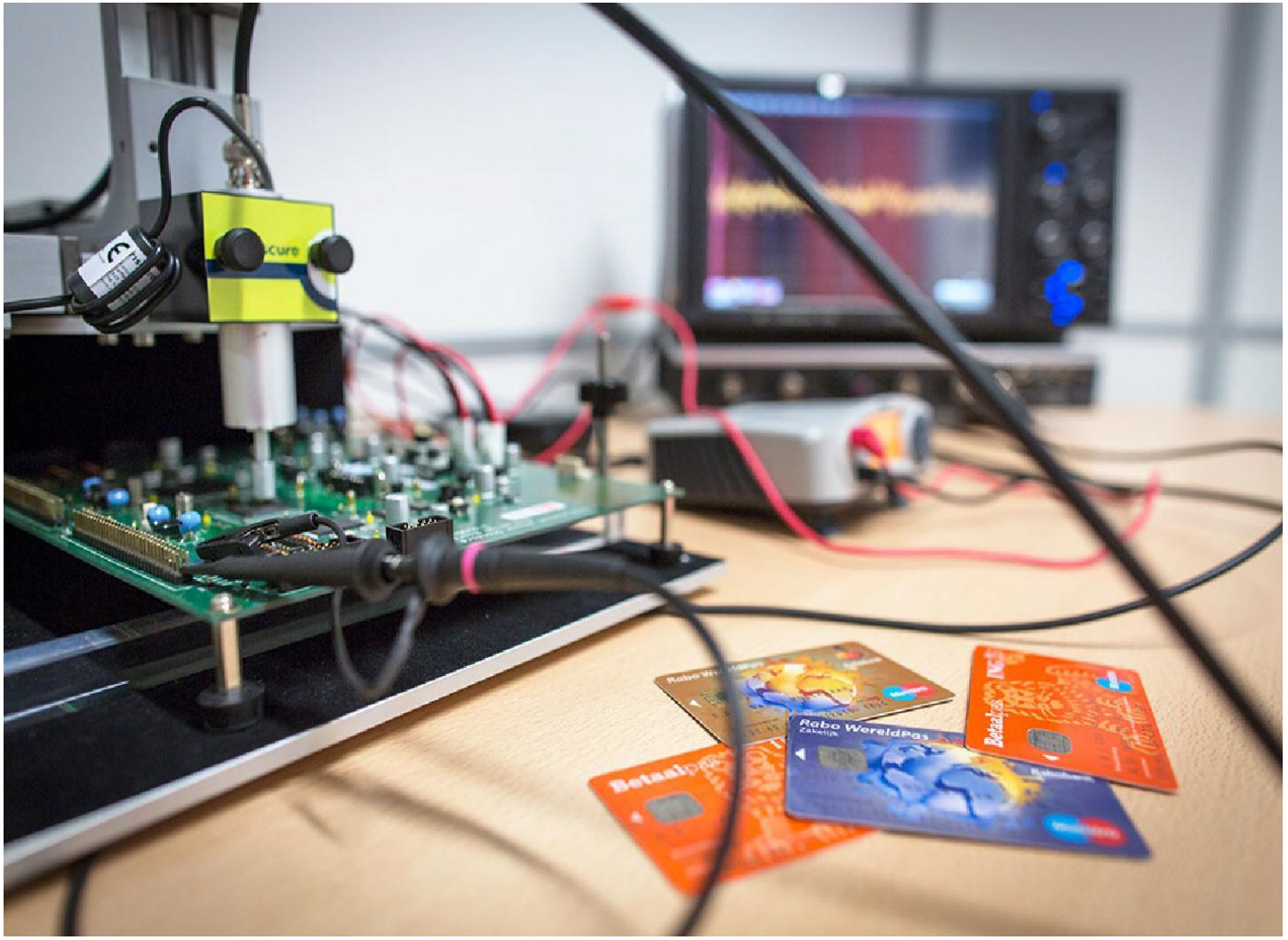


What is the key?

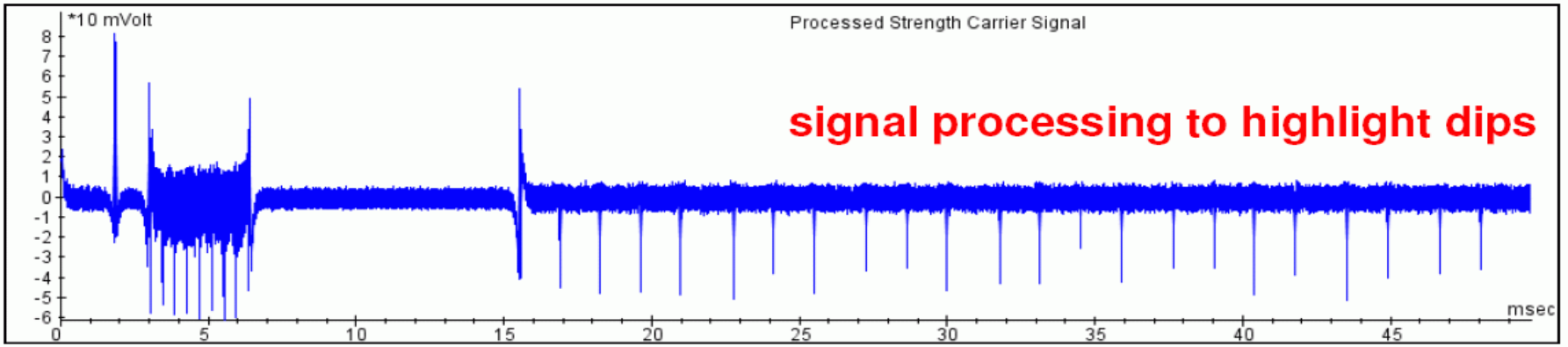
Analysis of the shape of signal in each round could reveal one bit of the key

Side-channel analysis using power consumption

Side channel analysis using EM radiation



Voorbeeld: sleutel raden adhv stroomverbruik



Hoe werkt RSA versleuteling?

Voor RSA decryptie moeten we x^e modulo p berekenen.

Naieve algoritme : `x * x * x * ... * x` berekenen in e stappen

Snelle algorimte: met herhaald kwadateren in log(e) stappen

Idee hierachter: bereken $x^{25} = x^{16} * x^8 * x^1$ van achter naar voren

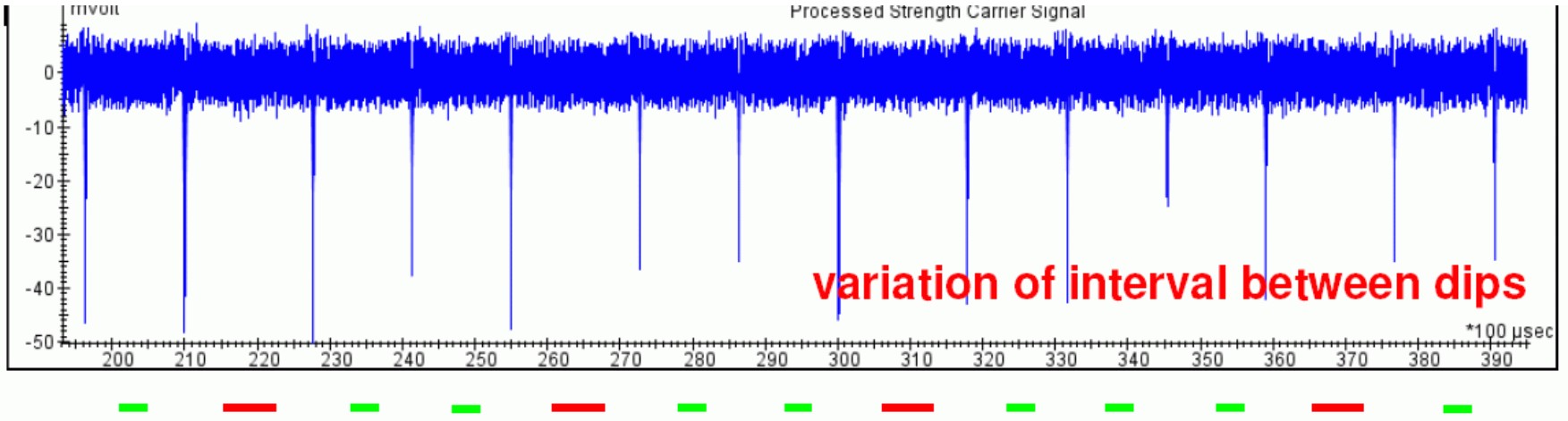
Pseudocode:

```
result = 1;  xi = x ;
for i = 1 to aantal bits in e do {
    if (i-de bit van e is 1) then result = xi * result
    xi = xi * xi; // xi is nu x tot de macht 2^i
  }
```

Merk op: elke iteratie doe je een kwadratering als bit 0 is

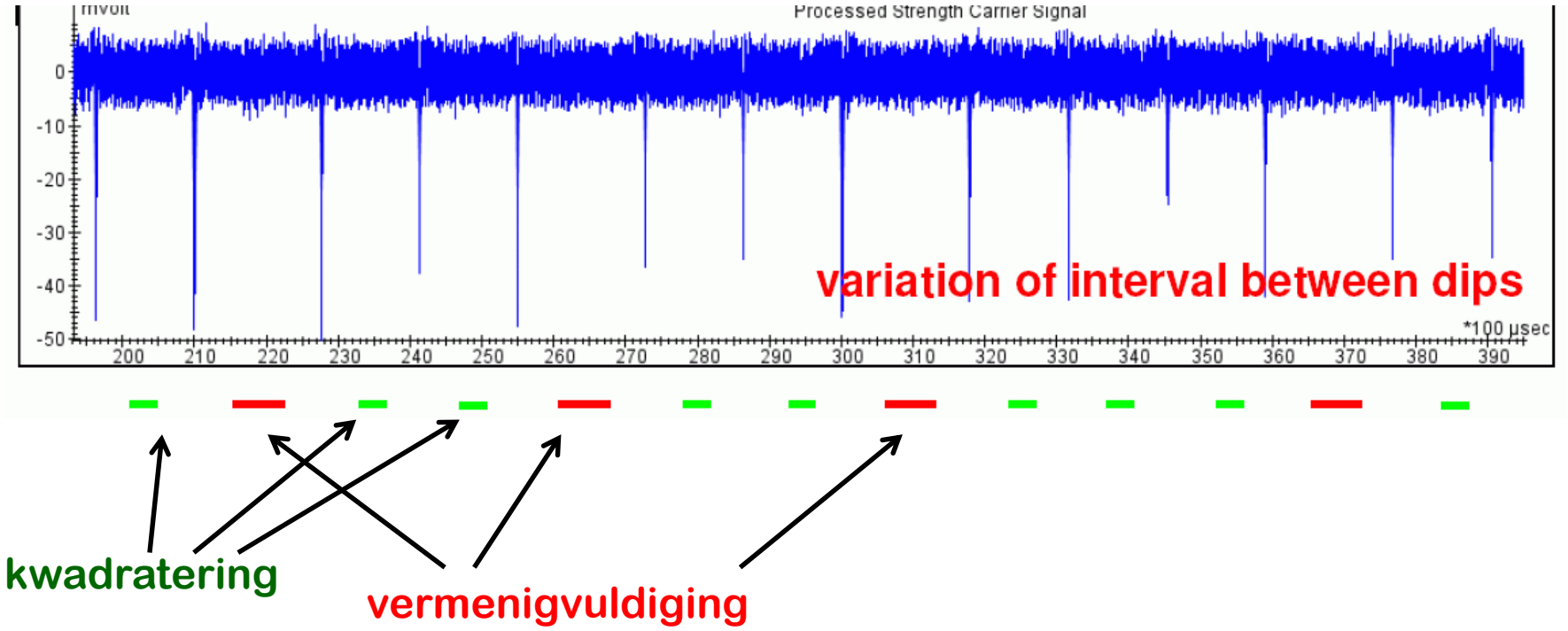
of een vermenigvuldiging en een kwadatering als bit 1 is

De sleutel van de trace aflezen?

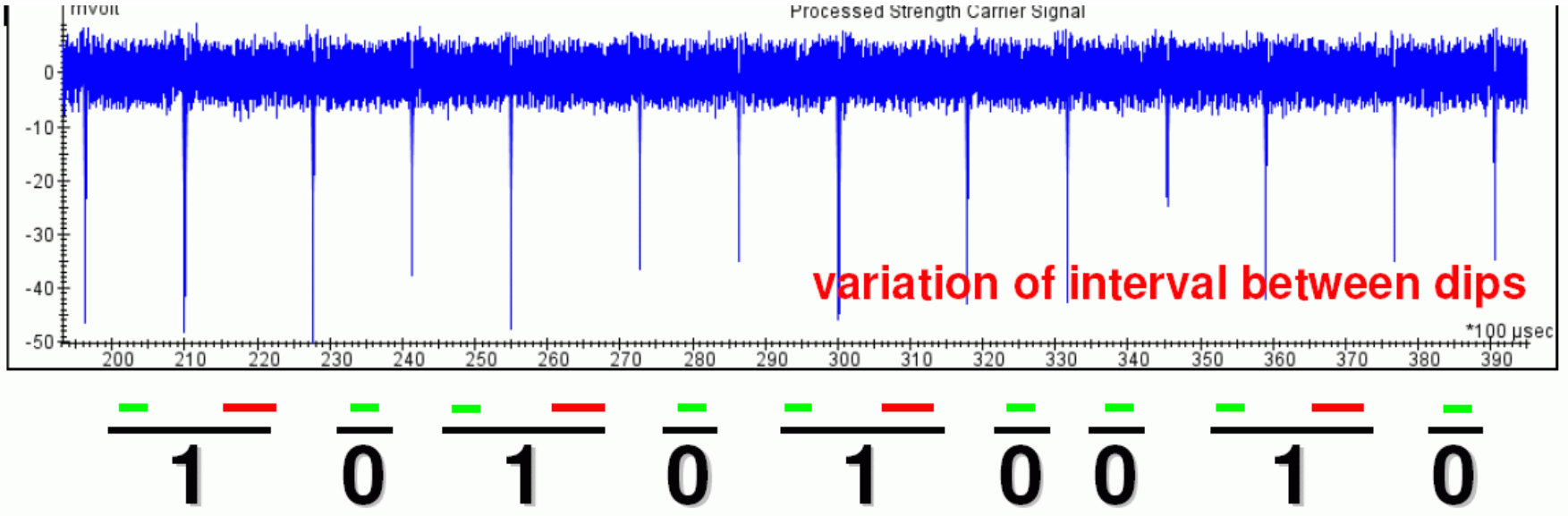


Wat zijn de *vermenigvuldigingen* en wat de *kwadrateringen*?

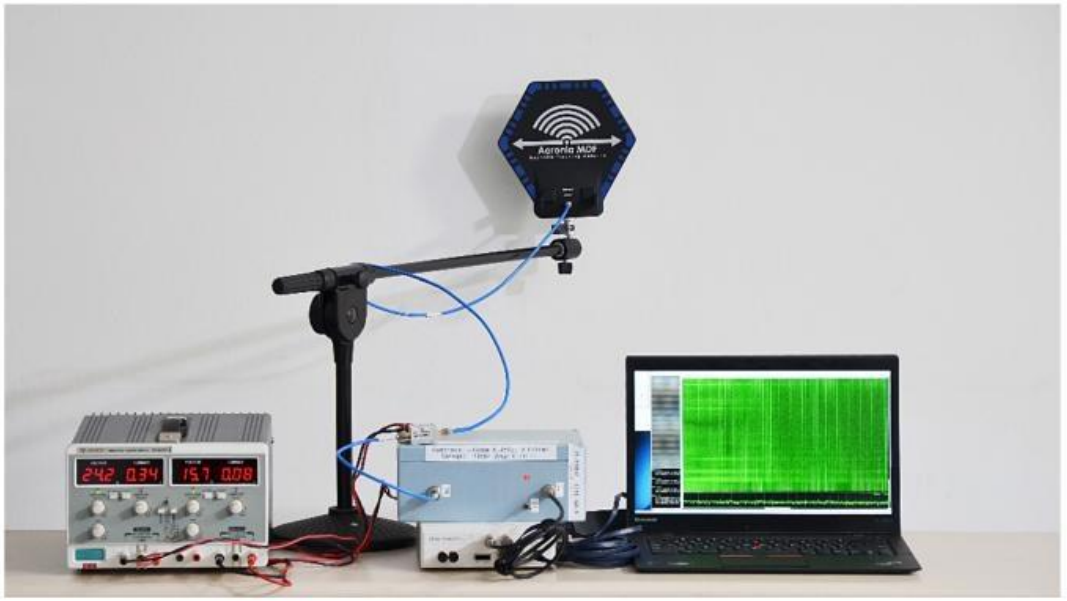
De sleutel van de trace aflezen?



De sleutel van de trace aflezen!



Not just for smartcards...



(a) Attacker's setup for capturing EM emanations. Left to right: power supply, antenna on a stand, amplifiers, software defined radio (white box), analysis computer.

(b) Target (Lenovo 3000 N200), performing ECDH decryption operations, on the other side of the wall.

[Daniel Genkin et al., ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs, RSA 2016, https://eprint.iacr.org/2016/129.pdf]

General observations about cyber security

Conclusions

- General trend: from prevention to better detection & response
- Technical security flaw not always a serious security risk.
  The real issue: can attackers find a good business model?
  - The bad news here: ransomware is a great business model for almost any security weakness
- Fundamental problems in improving security (incl. non-technical ones) :
  - How can we build software with fewer security vulnerabilities?
  - How to do good risk assessment to make rational security decisions?
  - How can we help end users to understand security measures & security risks?

Thanks for your attention