Cyber bank robbery

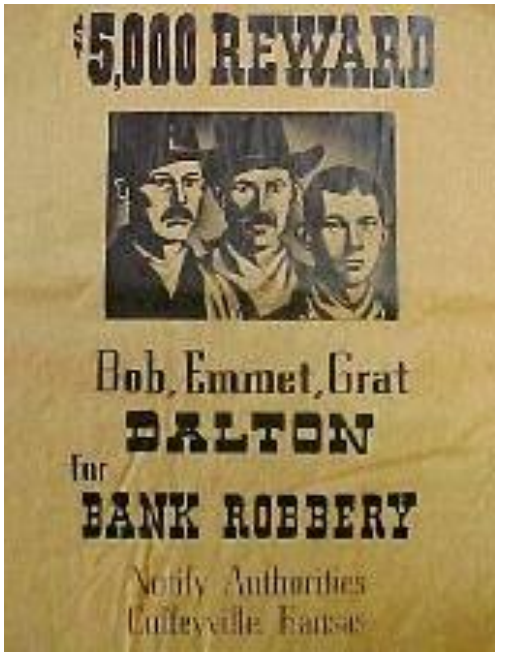
Erik Poll

Digital Security

Radboud University, Nijmegen, the Netherlands

Banken & cyber security

Banks a long-time favourite target of criminals



Also of *cyber* criminals

- **Some anecdotes & historical trends**
- **What can we learn from this?**

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**

These are no script kiddies, but serious organised crime

[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]

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

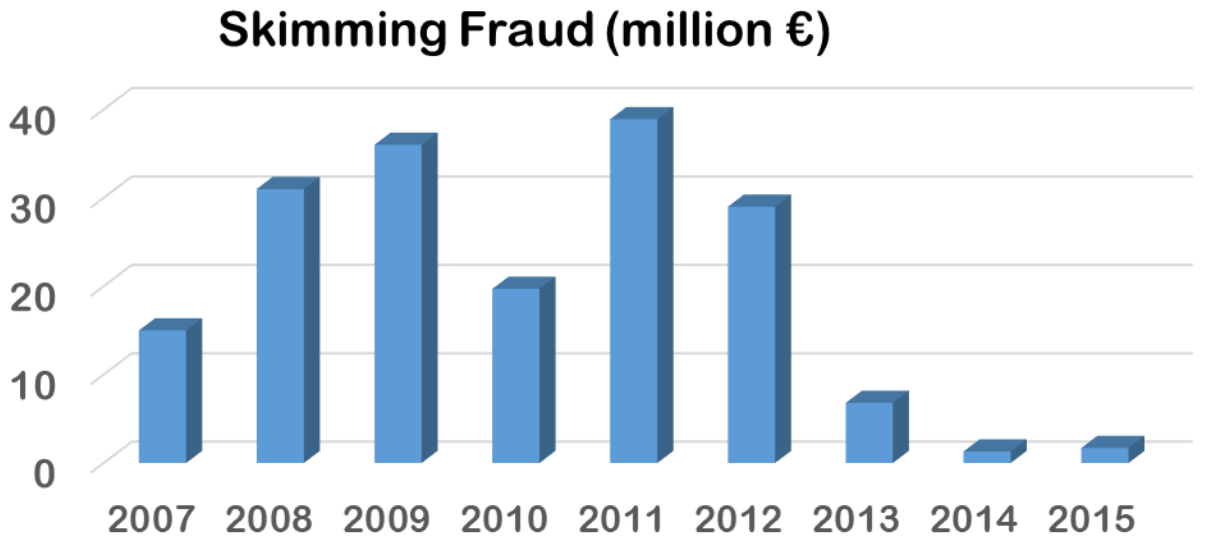
Fake cover
that makes
copy of the
magnetic stripe

More skimming equipment

Fake keyboard
to intercept PIN code

Fake cover
that copies magnetic stripe

Skimming 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

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

Does EMV chip  reduce skimming?

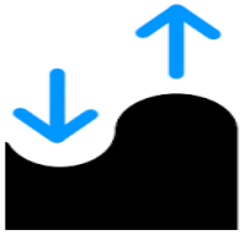
- UK introduced EMV in 2006

	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

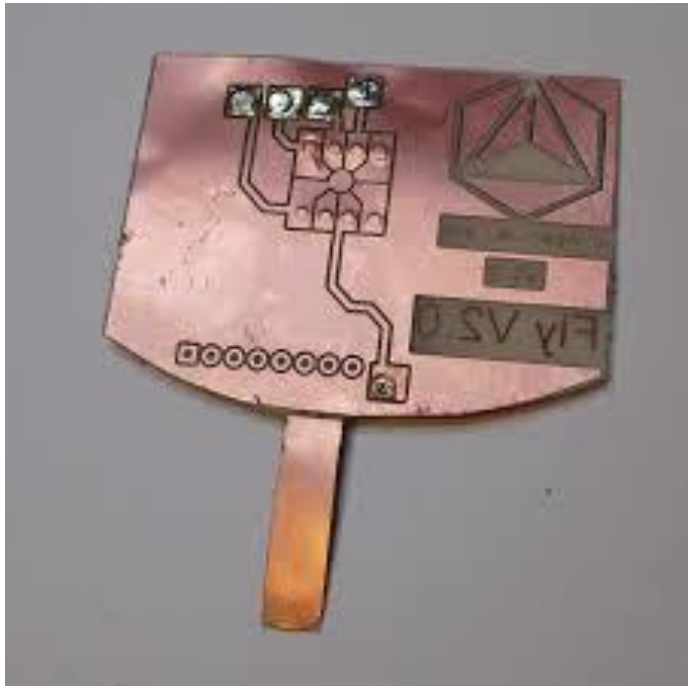


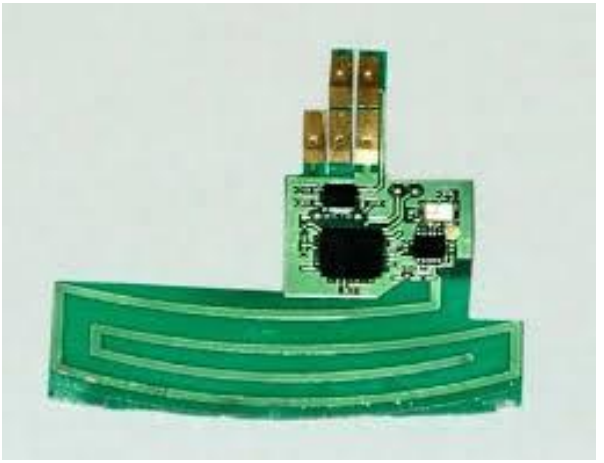
Recurring problem: BACKWARD COMPATIBILITY

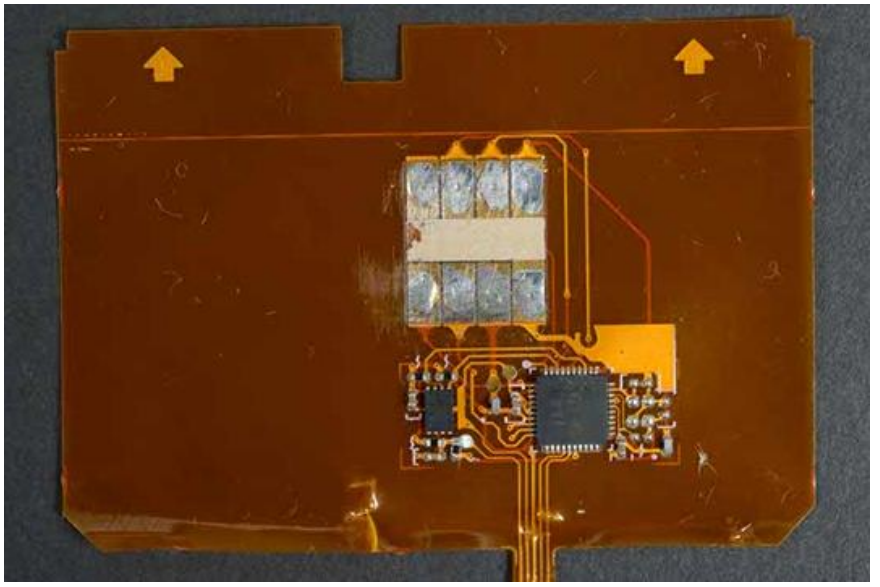
- In 2009, criminals put tampered card readers *inside* Dutch bank branches to skim cards
  - For *backwards compatibility*, the chip can report the mag-stripe data…
  - Both mag-stripe data and PIN code sent unencrypted from card to this reader
  - Criminals caught & convicted in 2011

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

Shims to eavesdrop on communication







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

More low-tech attacks: PHISHING

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

14 september 2015 13:55

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.

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 krijgt u uw nieuwe betaalpas volledig gratis. Normaliter brengen wij €24,99 in rekening voor een nieuwe betaalpas. Na dat u zich heeft aangemeld ontvangt u verdere instructies over het adres van het dichtstbijzijnde Rabo Recycle Point.

Let op: U kunt over twéé weken alleen nog gebruik maken van de nieuwe betaalpas.

Meld u hier aan voor uw online procedure

Heeft u meerdere betaalpassen? Dan raden wij u aan om uw betaalpassen in delen aan te melden, vergeet niet elke

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), ….**

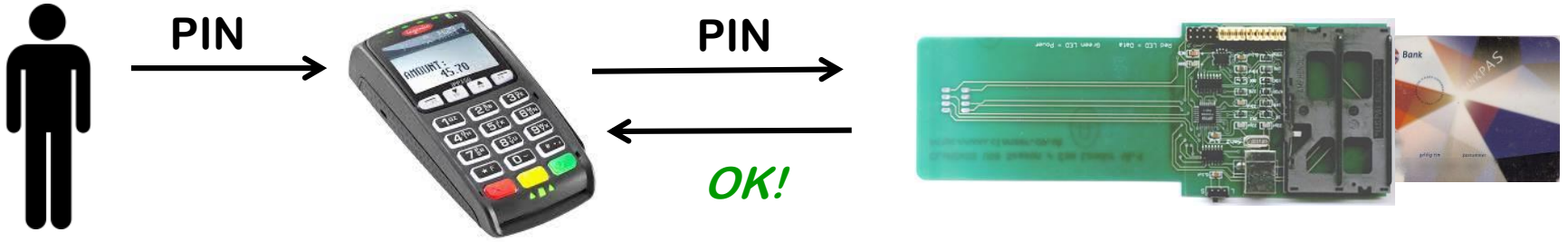
Sample sentence

"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."

Complexity: example protocol flaw

Terminal can choose to do offline PIN

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



The response of the card is *not authenticated*

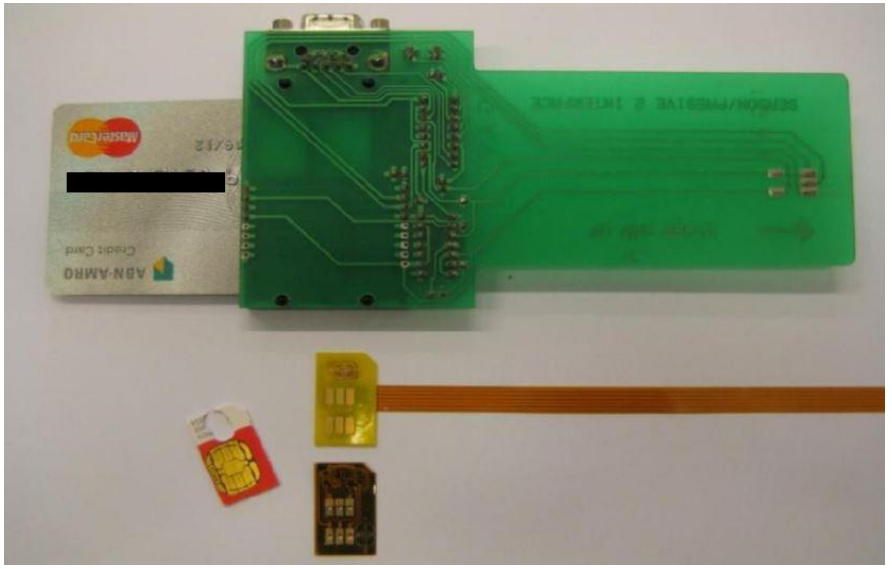
- ie. not cryptographically signed

so 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

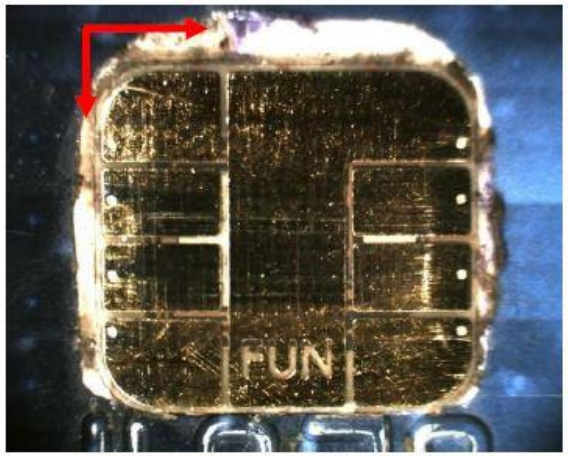
[Stephen Murdoch et al., *Chip & PIN is broken*, FC'2010]

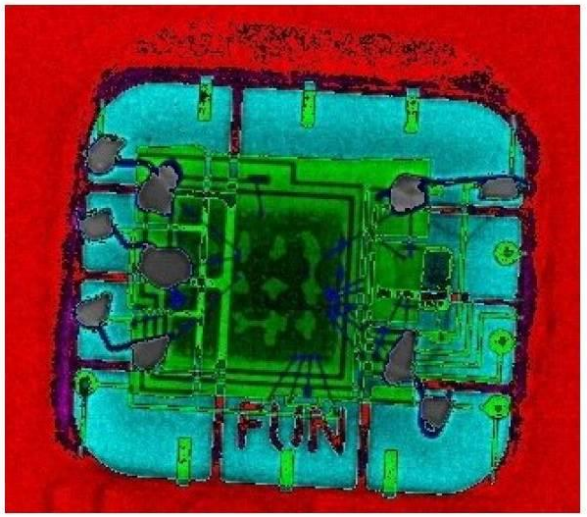
Our Man-in-the-Middle set-up

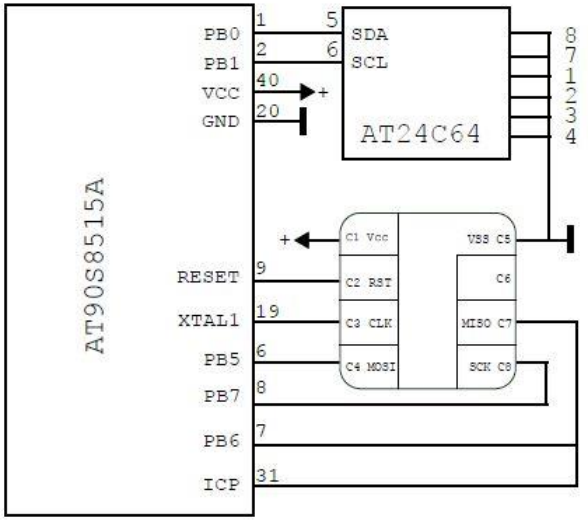


Criminal Man-in-the-Middle set-up

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



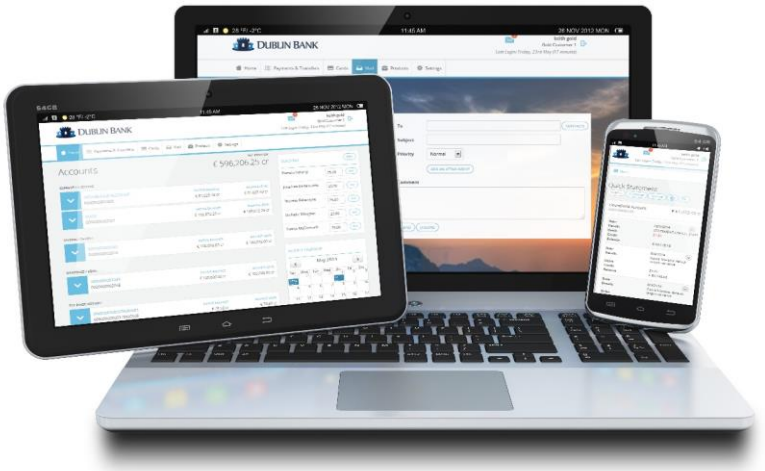




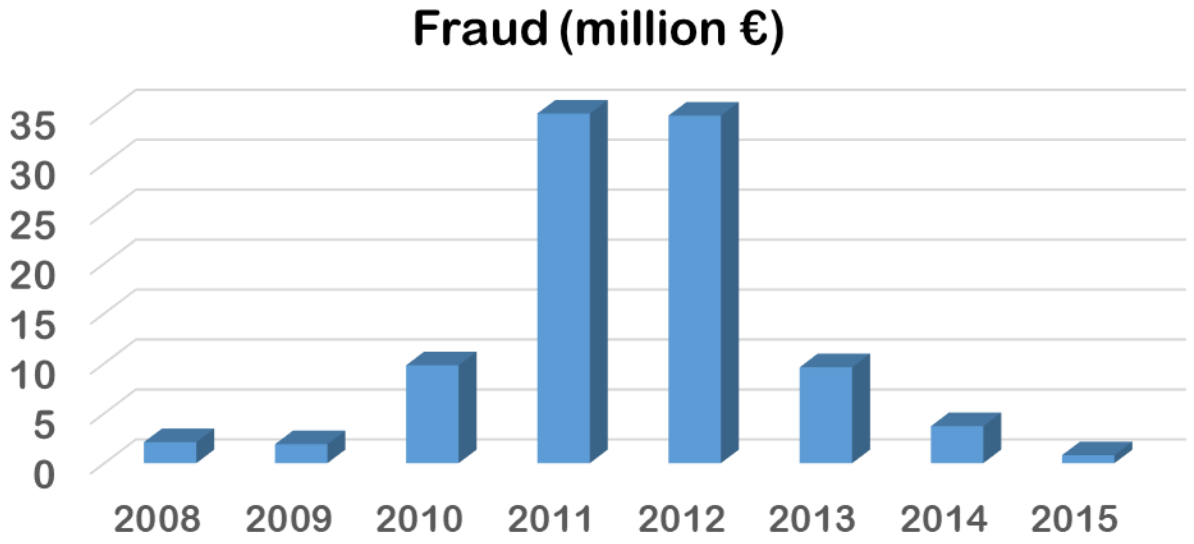
xray reveals green stolen chip under blue microcontroller

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

Internet banking



Fraud with internet banking in NL



[Source: NVB & Betaalvereniging]

Fraud under control thanks to

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

Strong authentication for online banking

- For authentication, most Dutch banks use stronger mechanisms than just username & password
  - TAN codes: one time passwords on a printed list
  - m-TAN: one time password received by SMS
  - hand-held reader that generates one-time code using bank card

  aka two-factor authentication

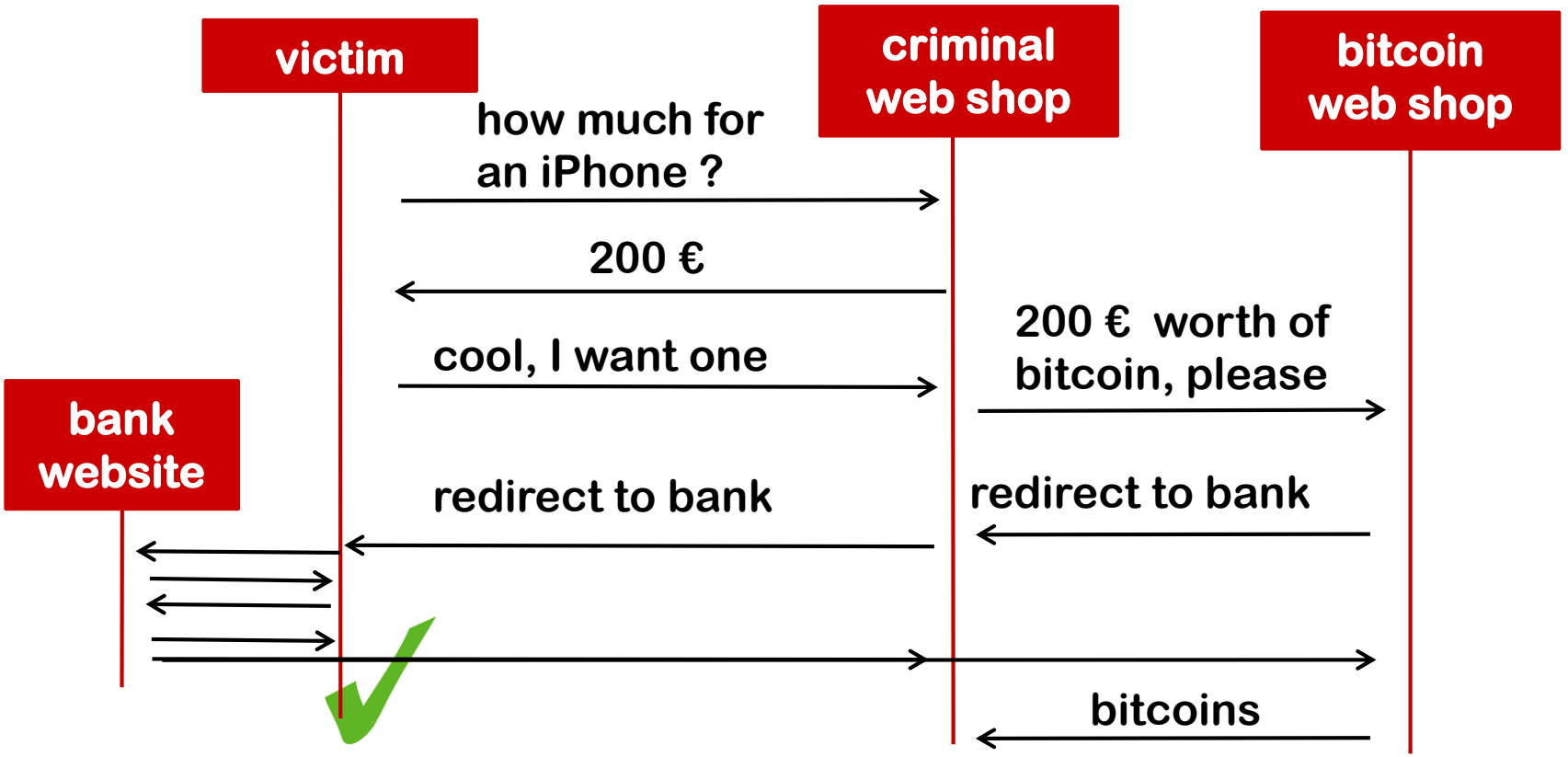
- Still, these mechanisms are not fool-proof…
  - eg. criminals have resorted to phoning people, pretending to be from the bank, to obtain these one-time codes

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 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 user not very informative, so user does not spot the attack
- Solution: better monitoring, and banks impose extra rules on bitcoin shops & online casinos for allowing internet payments

Example attack on internet banking (3)

- For banks that use m-TANs, ie. one time passwords sent by SMS, criminals can try to obtain a second SIM card for your phone number
- How?
  - *bribe someone at the Vodacom shop!*
- Countermeasure?
  - *bank can make deal with telco to be told about re-issued SIMs*

- Alternatively, phone can nowadays be hacked to steal one-time codes. This means the days of the m-TAN as a second factor are now numbered.

banking apps vs web browsers

- Dutch banks see fewer problems with banking apps than with online banking in web browser.
- Possible explanations:
  - Easier for criminal to lure victims to a malicious web site than get them to install a malicious app
  - Apps are updated frequently, and unique to every bank, so looking for flaws in these apps is less rewarding

Contactless payments

Contactless payments

Contactless version of EMV with bank card or NFC smartphone

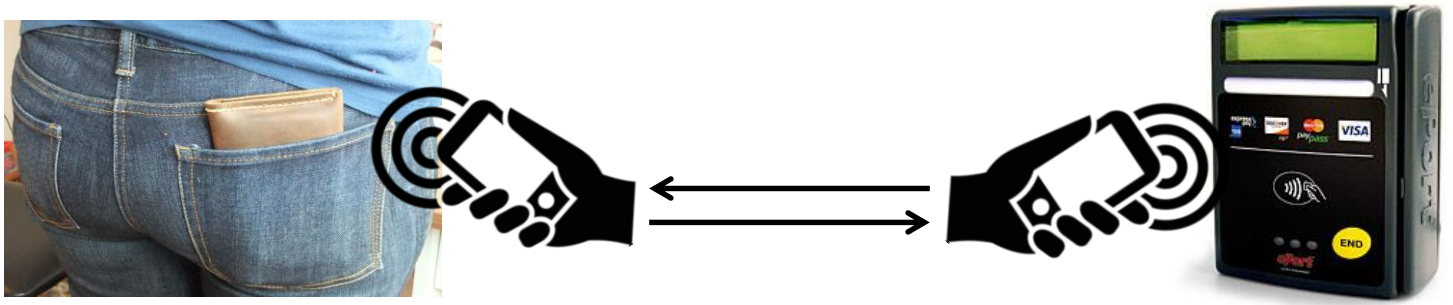
In Netherlands, for a maximum of 25 euro per individual transaction and a cumulative total of 50 euro until you use your PIN again.

Contactless payments

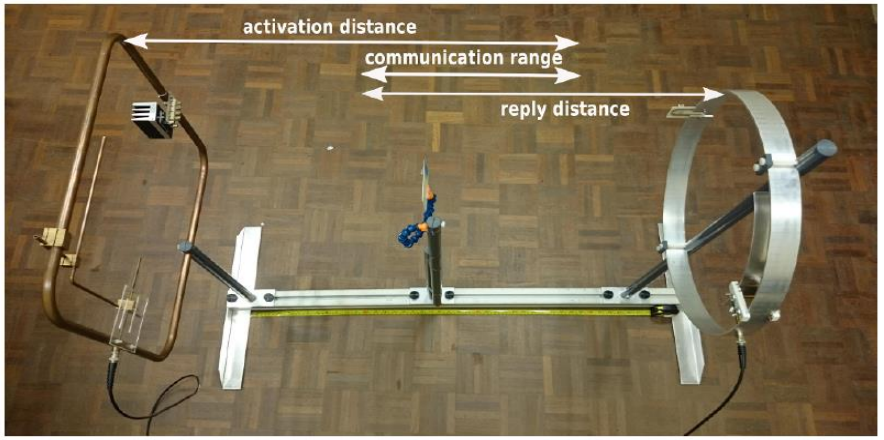
- ***Who uses a metal container to shield their contactless bank card?***
- ***Who has asked their bank to disable contactless payments for their card?***
- ***Who thinks that contactless payments without PIN is less secure than contact payment with PIN?***

Security of contactless payments

- It is not possible to clone a contactless card
- It is possible to do a relay attack



- But is there a good criminal business model? Probably not…
- Max. distance to activate card ≈ 40 cm



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

Risks of contactless 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…

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

Note: technical weakness in the security ≠ risk

where risk = likelihood x impact

Configuration flaws

Mistake on the first generation contactless cards issued in the Netherlands:

- **functionality to check the PIN code,**

  which should only be accessible via the contact interface 

  was also accessible via the contactless interface 

Possible risk for DoS attacks, rather than financial fraud?

Flaw discovered by Radboud students Anton Jongsma, Robert Kleinpenning, and Peter Maandag.

Software bugs

Contactless payment terminals of one manufacturer could be crashed with a legal – but unusual – input

- Probably due to a buffer overflow
- Bug might be used for more interesting attacks than just Denial-of-Service, eg. to get malware on the terminal

[Jordi van den Breekel, A security evaluation and proof-of-concept relay attack on Dutch EMV contactless transactions, MSc thesis, 2014]

- The input format of smartcard terminals is very simple:
  - how can you implement this wrong?
  - if you do, how do you miss it in testing?

Command APDU						
Header (required)				Body (optional)		
CLA	INS	P1	P2	Lc	Data Field	Le

- Apparently, certification schemes for terminals such as are not testing for such basic flaws…

Conclusions

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
- Some silly security flaws by reputable companies & vendors
  - Who is *really* taking responsibility for the security ?
    - Individual banks? Their suppliers? 3rd parties doing certification? MasterCard & Visa, who also approve vendors & certifiers?
  - How much security is just Cover-Your-Ass security?

Why banking security is easy!

- Banks can measure attacks & quantify their costs euros, so
  - Trend in attacks can be monitored
  - Success of defensive measures can be measured
  - This provides a rational basis for security decisions

- In other industries this is MUCH harder
  - Eg for critical infrastructures or hospitals:
    - How much can cyber protection of the electricity grid cost?
    - How much can patient privacy cost?
  - Ransomware may play a 'useful' role here…