Outline

Introduction

A bit about bitcoins & blockchains

PSD2

Conclusions
Where we are, so far

Introduction

A bit about bitcoins & blockchains

PSD2

Conclusions
### Financial crime in NL in M€ (Source: Betaalvereniging)

<table>
<thead>
<tr>
<th>Activity</th>
<th>'92</th>
<th>'10</th>
<th>'11</th>
<th>'12</th>
<th>'13</th>
<th>'14</th>
<th>'15</th>
</tr>
</thead>
<tbody>
<tr>
<td>bank robbery</td>
<td>570</td>
<td>26</td>
<td>7</td>
<td>4</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>internet banking</td>
<td>—</td>
<td>10</td>
<td>35</td>
<td>38</td>
<td>9.6</td>
<td>4.7</td>
<td>3.7</td>
</tr>
<tr>
<td>bankcard skimming</td>
<td>—</td>
<td>20</td>
<td>40</td>
<td>29</td>
<td>6.8</td>
<td>1.3</td>
<td>±0</td>
</tr>
</tbody>
</table>

**Remarks:**
- You’re an **old-school loser** if you’re still planning a career as bank robber
- **Bad guys have gone digital**, in fraud, blackmail, sabotage, espionage
- New forms of financial fraud constantly appear, like: asking people to send in their bank card, or attacking cash machines
  - total fraud level is a bit higher in 2015 than 2014
“In five years half of all crimes are carried out by cybercriminals”

PG Gerrit Verburg, Nieuwsuur 15 juni 2016
Warfare has gone digital: a picture says it all

American Cyberattacks On Iran - 08 Jun 2012
Image 3 of 19

(© Herald Tribune)
Wars and Sciences

- **WWI** was the chemists’ war, with the use of poisonous gases

- **WWII** was the phycists’ war, with the atomic bomb

- **WWIII**, if ever, will be the computer scientists’ war
Computer security is interdisciplinary

- **Mathematics**: cryptology as basic toolkit for encryption, signing, authentication, etc.
- **Computer security**: the software, hardware, networks that make things work
- **Management / economics / psychology**: which incentives work?
- **Law / ethics / politics**: what is/should be allowed, esp. against cybercrime and for dataprotection
Societal relevance

Traditional view:
- computer scientists are architects of the digital world

Modern view:
- computer scientists are architects of the social world

Computer security and privacy issues can make or break developments in:
- communication
- transportation
- health care
- finance & insurance
- government etc.
What is computer security about?

Computer Security is about regulating access to (digital) assets

Key issues

- assets: the valuables that need protection
  - Eg. company secrets, or personal data (privacy)
- regulating access: involves
  - identification: who are you? / what are your attributes?
  - authentication: how do you prove this?
  - authorisation: what are you allowed to do

Implicitly there is a malicious attacker that is trying to get unintended access and to undermine your (computer) system
Own/group involvement in ICT-security & finance

- Security of bank cards: move from magnetic stripe to chip
  - now also: relay attacks on contactless payment cards

- Security of internet banking
  - e.g. protocol error discovered in ABN AMRO’s random reader
  - authentication of customers and digital signatures

- Bitcoins and blockchains — see later
  - topic of nov.’17 blog at ibestuur.nl

- Payment Service Directive 2 (PSD2) — see later
  - topic of sept.’17 blog at ibestuur.nl

Betaalvereniging is paying a part-time (0.2) professorship on financial information security in Nijmegen — occupied by Eric Verheul
Where we are, so far

Introduction

A bit about bitcoins & blockchains

PSD2

Conclusions
Bitcoins in action

Some relevant webpages:

- new, unconfirmed transactions or bitcointicker
- bitlisten.com for an artistic visualisation
- bitcoin value chart
- overview of various cryptocurrencies
Bitcoin transaction (commonly denoted as: tx)

- **inputs:**
  - earlier transactions received by the payer

- **outputs:**
  - beneficiaries (payees) of this transaction

- The sum of the bitcoin amounts in the inputs must **exceed** the sum of the amounts in the outputs
- The difference is the **transaction fee**, which is for the successful “miner” (see later)
  - In practice a non-zero fee is needed to get processed
Bitcoin transaction arithmetic

Suppose that Alice wants to pay 5 BTC to Bob, ...

...and that Alice has been payed herself in two previous transactions, one with 2.5 BTC and one with 4 BTC.

How to proceed?

For the 5 BTC payment to Bob, Alice can use:

- **inputs**: both these transactions, of 2.5 BTC and 4 BTC
- **outputs**: 5 BTC to Bob, and 1,49999 BTC to herself
- The transaction fee is thus:

\[(2.5 + 4) - (5 + 1,49999) = 0.0001\text{ BTC}\]

if 1 BTC = 8000€, this fee is 80 eurocent.
Transaction inputs, in a diagram

(source: Ken Shirriff’s blog, feb. 2014)
Bitcoin mechanics (high level)

▶ A Bitcoin address looks like an arbitrary number, but is a hash of a public cryptographic key

▶ A user may have/generate/use multiple addresses
  • the addresses are all public, but you can hide the link between you and your addresses (eg. via mixers)
  • this provides (some) transaction privacy
  • using multiple addresses gives an additional level of obfuscation

▶ Basic cryptographic operations, like signing and hashing, ensure:
  • only owners of addresses can transfer from these addresses
  • a link between the current and previous transactions

▶ So-called miners collect unconfirmed transactions and put them in a block, that gets added to the blockchain
  • building a block involves solving a mathematical puzzle
  • this puzzle requires huge computational resources (and energy)
  • the winner gets the transaction fees, plus a fixed amount
Some general remarks

▶ Bitcoin is far from being “green”
  • Recent claim: energy consumption of one bitcoin transaction is enough for a normal house for one week

▶ Public authorities have difficulty coping with Bitcoin
  • mixed reactions (banning, tolerating, ignoring)
  • NL attitude (DNB/AFM): “there are risks”
  • the value is extremely volatile
  • transaction speed is too limited (max. 7 per second)

▶ Since Bitcoin hundreds of other cryptocurrencies have emerged
  • most well-known alternative is Ethereum
  • they have given rise to Initial Coin Offerings (ICO’s)

▶ Not so much Bitcoin, but the underlying blockchain technology has become a complete hype
  • unsuitable for personal data, not only because of privacy
  • but also: data is not removable, which is legally required
Where we are, so far

Introduction

A bit about bitcoins & blockchains

PSD2

Conclusions
Own involvement in PSD2

▶ Supervision of master thesis on this topic in 2016 [link]
▶ Invited presentation at DNB, at an internal PSD2 discussion session for board & directors (4/9/17)
▶ Online blog at ibestuur.nl, with title: PSD2, een Europese strategische blunder (published 12/9/17)
▶ Appearance in consumer programme Radar about PSD2 (23/10/17)
▶ Participant in expert hearing of Financial Committee in Parliament (15/11/17)
  • Opening statement: welke malloot heeft dit verzonnen?

Inbetween: various informal discussions with bank representatives.
Essentials of the PSD2 regulation (and abbreviations)

- Part of the European legal framework for the financial industry
  - intended to create a level playing field for FinTech startups
- Two new roles:
  1. Account Information Service Providers (AISP)
  2. Payment Initiation Service Providers (PISP)
- Banks are called: account servicing payment service providers (ASPSP)
  - they are obligated to cooperate with SPs = AISPs & PISPs
  - without discrimination and free of costs
- PSD2 contains accompanying requirements wrt. security of online payments and account access: “regulatory technical standards” (RTS)
- Structure of supervision on SPs:
  - EBA at European level — including security & data protection
  - National bank (DNB) issues permits
  - who have to cooperate with relevant authorities (AP, AFM, ACM)
Privacy is keeping information in context (Helen Nissenbaum)

► We naturally live in different contexts
  ● home, work, sports club, in church, with friends . . .

► We naturally want to keep information in context
  ● what we tell to our doctor should not end up in a supermarket

► People get upset when contextual integrity is broken
  ● recall anger: about selling customer financial data (ING), about speeding data ending up at the police (TomTom), about school children’s performances in online tests ending up at publishers

► When explained like this, almost everybody cares about privacy

► The Google’s and Facebook’s of this world make us use the same identifier everywhere or track us via Like and cookies
  ● they break-up contexts, and destroy our basic privacy intuitions
  ● Mark Zuckerberg: “Having two identities for yourself is a lack of integrity” 😞😞😞
PSD2 and data protection

Business models of FinTech are based on personal data processing
- data protection regulation is thus highly important
- exit plan with data deletion now required by DNB

GDPR requirements that are most relevant for PSD2:
- user consent, based on objective, understandable information
- purpose binding: data usage for requested purposes only
- data minimisation: only data which is directly relevant to the service may be used

Security breach notification to ‘competent authority’ (NCSC?)
- but also NL data breach notification (to AP) applies
Some problems with PSD2

(1) The idea is to support “friendly” and innovative FinTech’s
   • in practice, the big-five will benefit most
   • they get free payments and valuable consumer data for free!
   • strategic blunder: also US social media companies should be forced to open up.

(2) PSD2 parties (PISP + AISP) may seek access ‘via user portal’
   • Germany payment service Sofort requires user’s PIN code !!
   • lame regulation compromise: only allowed as “fall back”
   • much confusion, which will be exploited by criminals

(3) Who registers consent how?
   • AISP can say to bank: this customer of yours has given me consent: now you must cooperate and hand over data
   • banks want consent registration via their authentication means
Problems with PSD2, continued

(4) Who determines what is a service?
- can Google use your payment data to personalise maps: show only those restaurants that (Google thinks that) fit your budget?
- personalised advertisement and pricing may well lead to higher prices

(5) Personal “consent” to open up your bank account may be not be a free choice at all:
- e.g. when you want mortgage advice
- or get Visa, e.g. for entering the US

(6) Consent in itself is a very problematic mechanism in itself
- many people agree to anything, just to be able to proceed
- more consumer choice mostly benefits big-IT !!!
- still, free choice remains a powerfull mantra, just like innovation
Problems with PSD2, continued further

(7) National permits are valid throughout EU
   • cowboys will seek entry point with least requirements
   • intelligence agencies will also ‘organise’ permits

(8) Even I can see that free-of-cost requirements are economic madness
   • maintaining secure payment infrastructure does cost money
   • carefully built collections of personal data are very valuable

(9) In general, inherent tensions between PSD2 and GDPR
   • problematic for banks; little guidance from regulators so far
   • will lead to uncertainty and litigation
Where we are, so far

Introduction

A bit about bitcoins & blockchains

PSD2

Conclusions
Final remarks

➤ **Computer security & privacy** are now essential for the financial sector
  • not only for protection of existing infrastructure
  • but also for new cryptocurrencies and services

➤ **Blockchain** is the **hype of the century**
  • too much **bluff your way into blockchain**
  • proper knowledge and critical attitude are badly needed

➤ **PSD2** is an epic European **shoot-in-the-foot**

For more positive use of technology, see: [privacybydesign.foundation](https://privacybydesign.foundation)