mobile business

Masters Seminar
2015

Privacy, security and fraud detection solutions for communication services

Agenda

1. Your Team
2. Organizational Issues
3. Introduction to the Topics
4. Distribution of Topics
5. Scientific Working
7. Your Questions

Your Team
Prof. Dr. Kai Rannenberg

- **Holder of the Chair of Mobile Business & Multilateral Security**
- Research Interests
  - Mobile applications and Multilateral Security in e.g. Mobile Business, Mobile Commerce, Mobile Banking, and Location Based Services
  - Privacy and identity management, communication infrastructures and devices,
such as personal security assistants and services
  - IT security evaluation and certification

Ahmed Yesuf

Research Assistant

Research Focus:

- Validation and evaluation of security solutions
- Metrics to evaluate security approaches

Research areas:

- System security and modelling
- Secure software development
- Design and requirements engineering

Project involved:

- TREsPASS (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security)

predict
prioritise
prevent
TREsPASS

Stephan Heim

Research Assistant

Research Interests

- User Acceptance of Social Network Services in Multinational Enterprises
- Privacy in Enterprise Communities
- Privacy in Mobile Communities

Completed Projects

- **P**rivacy and **I**dentity Management for **Co**mmunity **S**ervices (PICOS)
- Attribute-based Credentials for Trust (ABC4Trust)
- Industry Projects

2. Organizational Issues

Organizational Issues

Language

- Course Language: English.
- Seminar paper and presentation slides have to be delivered in English (except Seminar Papers marked with GER).
- Presentations have to be held in English.

Organizational Issues

Deliverables

Seminar Paper

- Scientific paper presenting your research question, methodology, results, and the used literature.
- Has to be structured according to scientific guidelines.
- Around 20 pages (excluding references).
- Deadlines:
  - Draft version: 01.06.2015 (e-mail, editable document)
  - Final Version: 08.06.2015, 3 PM (printed + e-mail)

  → Deliver to Elvira Koch, RuW 2.257
- Template available: Link (Please use the citation style from WIRTSCHAFTSINFORMATIK: Link or MISQ Link)

Presentation

- Slide set summarizing your results and research methodology.
- Presentation time: 30 min + 15 min discussion
- Format: PowerPoint or OpenOffice Impress
- Deadline final version: 18.06.2015, 23:59 (CEST) (via e-mail to your supervisor)

Organizational

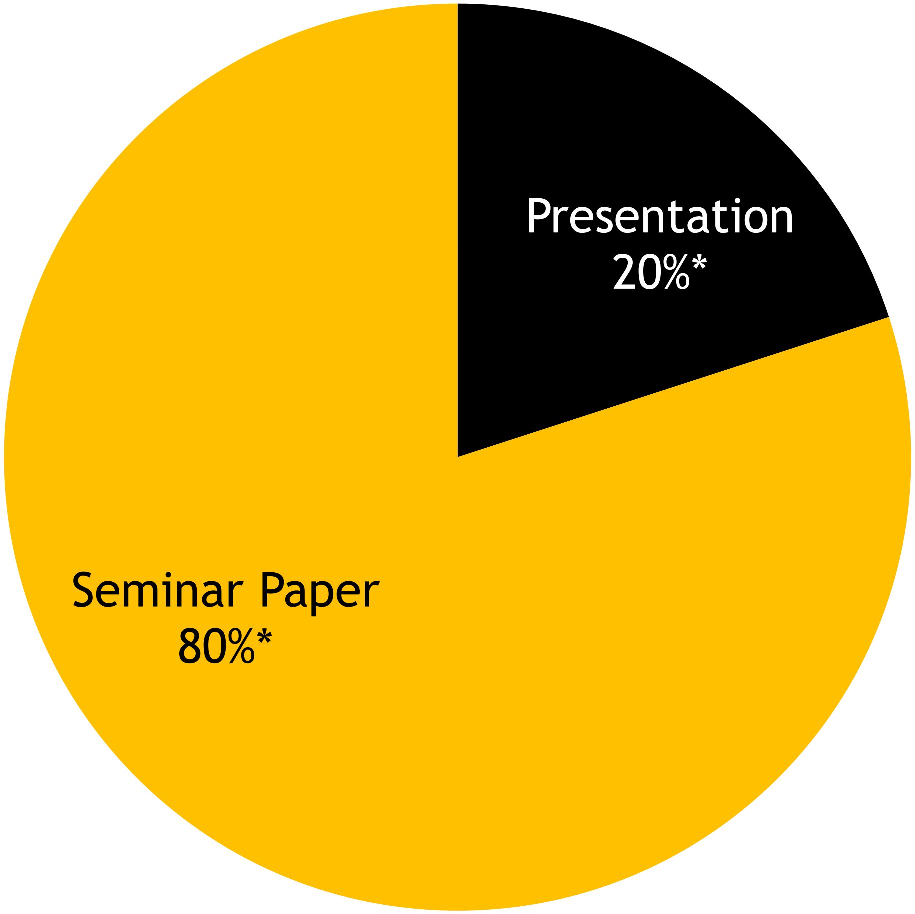
Dates & Rooms

Time	Room	
14.04.15, 10:00-12:00	2.202 (RuW)	Introduction & Assignment of Topics
25.06.15, 09:00-18:00	2.202 (RuW)	Presentations (Day 1)*
26.06.15, 09:00-18:00	2.202 (RuW)	Presentations (Day 2)*

* The agenda will be sent to you a few days in advance

Organizational Issues

Final Grade



*Participation in both parts is required for the successful completion of the seminar.

Organizational Issues
Contact

For organizational issues:

seminar@m-chair.de

For topic-specific issues:

Ahmed.yesuf@m-chair.de

or

Stephan.heim@m-chair.de

3. Introduction

Intro

PART I: FRAUD PREVENTION TECHNIQUES FOR TELECOM COMPANIES

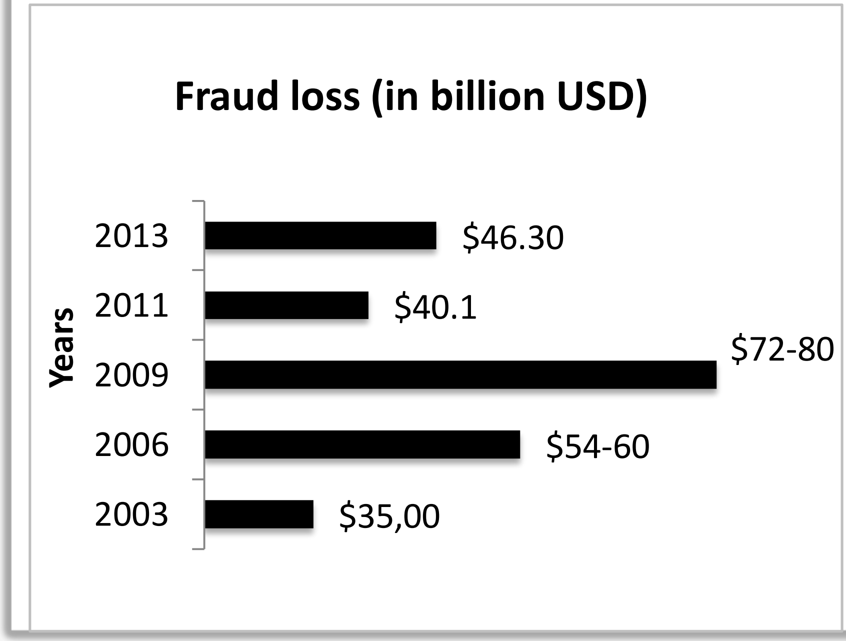
Introduction

Telecommunication services

- Telecommunication services:
  - Voice mail, data services, audio/video tex services,
  - Fixed telephone services
  - Cellular mobile telephone services
  - Carrier services
  - Provision of call management services
  - Data transmission services

Introduction
Telecommunication Fraud

- The use of telecommunication services or products with no intention of payment. [1]
- Approximately $46.3 billion (USD) lost in 2013 (up to 15% increase from 2011)



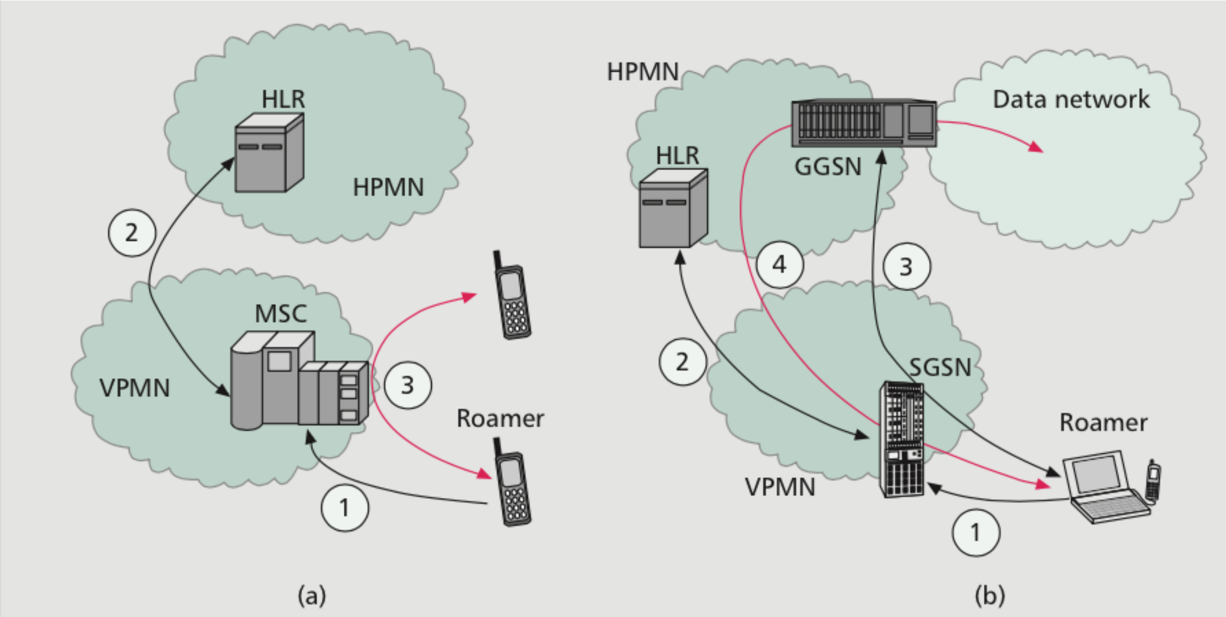
- $4.42 Billion (USD) – PBX Hacking
- $3.62 Billion (USD) – VoIP Hacking
- $6.11 Billion (USD) – Roaming Fraud

[1]

Roaming Fraud

"roaming is the ability of customers to use their mobile phones or other mobile devices **outside the geographical coverage** area provided by their normal network operator." – The GSM Association

- Roaming services: voice, data, MMS, and SMS



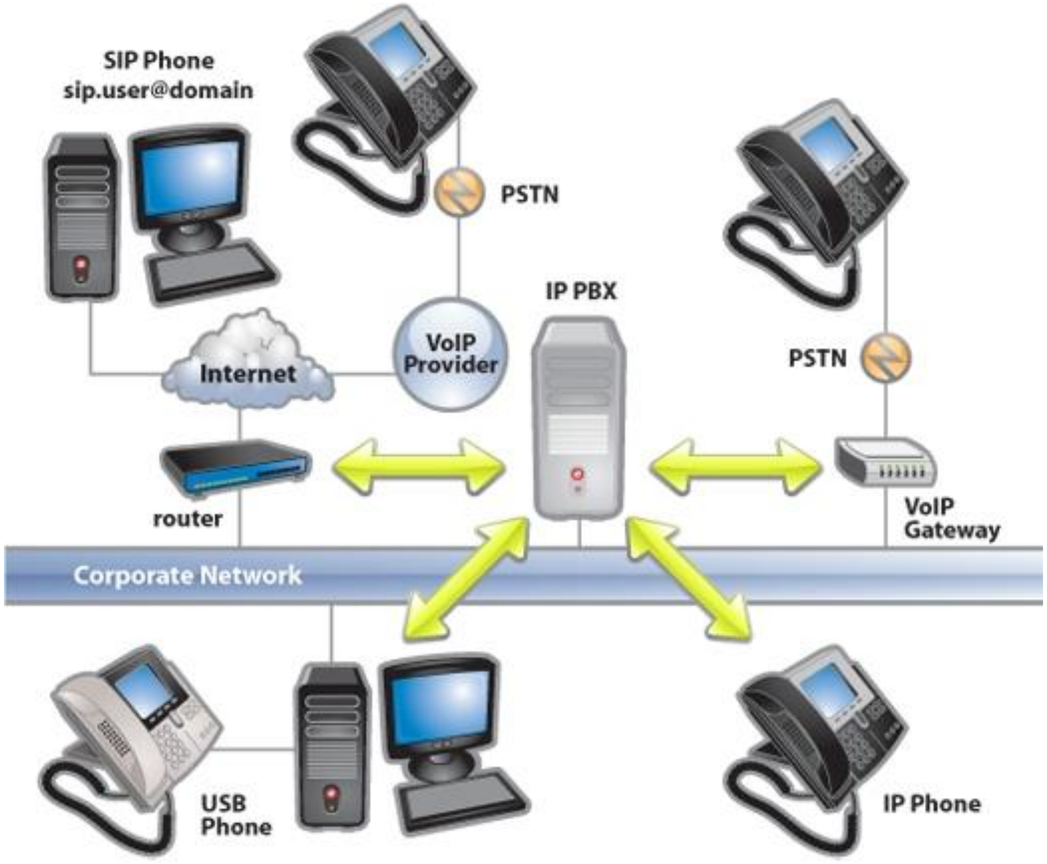
[2]

Roaming Fraud …

- Fraud based on technical network factors
  - Interoperability
  - Information transmission delays
  - Configuration flaws
- Fraud based on other business flaws
  - Subscription fraud
  - Internal frauds
  - M-commerce
  - Copyright and hacking

PBX fraud

- PBX (Private Branch Exchange): a private telephone network within an enterprise.



Types of PBX

1. TDM (Time Division Multiplexer)
2. IP PBX
3. Hybrid PBX

PBX fraud…

- NEC Nederland BV (“NEC”), the Dutch branch of NEC Corporation which is a worldwide provider of IT and communication solutions, uses voice services provided by KPN BV (“KPN”), a Dutch telecom provider.
- Unauthorized parties got access to the data lines via a badly secured NEC PBX device and set up a dial up service through which telephone traffic with East Timor took place. KPN invoiced NEC for the costs involved, in the sum of ***EUR 176,895***.

[3]

Topics

- Topic 1: Actors involved in IP PBX fraud
  - Who (person, software or organisation) are involved in committing IP PBX fraud?
  - Example scenarios when necessary
- Topic 2: Potential emerging risks of IP PBX system
  - What are the risks of current IP PBX systems?
  - One or two scenarios two show the risk
- Topic 3: Potential emerging risks of Roaming
  - What are the risks of current Roaming?
  - One or two scenarios to show the risks

Topics…

- Topic 4: The economic impact of roaming fraud to operators
  - discussion on one or two scenarios
- Topic 5: The economic impact of roaming fraud to the subscribers
  - discussion on one or two scenarios
- Topic 6: The impact of roaming fraud on the reputation of operators
  - discussion on one or two scenarios

Topics...

- Topic 7: Who is legally liable for damage accused by IP PBX fraud?
  - Discussion on a or two scenarios
- Topic 8: Requirements (considerations) of an IP PBX fraud prevention systems (approaches)
  - What will a prevention system (approach) has to fulfil in order to prevent from fraud?
- Topic 9: Requirements (considerations) of a Roaming fraud prevention systems (approaches)
  - What will a prevention system (approach) has to fulfil in order to prevent from fraud?

Intro

PART II: FRAUD SCENARIOS IN MOBILE WALLET AND BITCOIN ECOSYSTEMS

Bitcoin
What is a Bitcoin?

- Bitcoin is a digital currency that can be exchanged for goods and services.
- Bitcoins cannot be printed or physically made. They must be generated through computerized methods.
- Dezentralized: Bitcoins are not regulated by any government or banking institution

Bitcoin
Fraud scenarios

Consumers risks

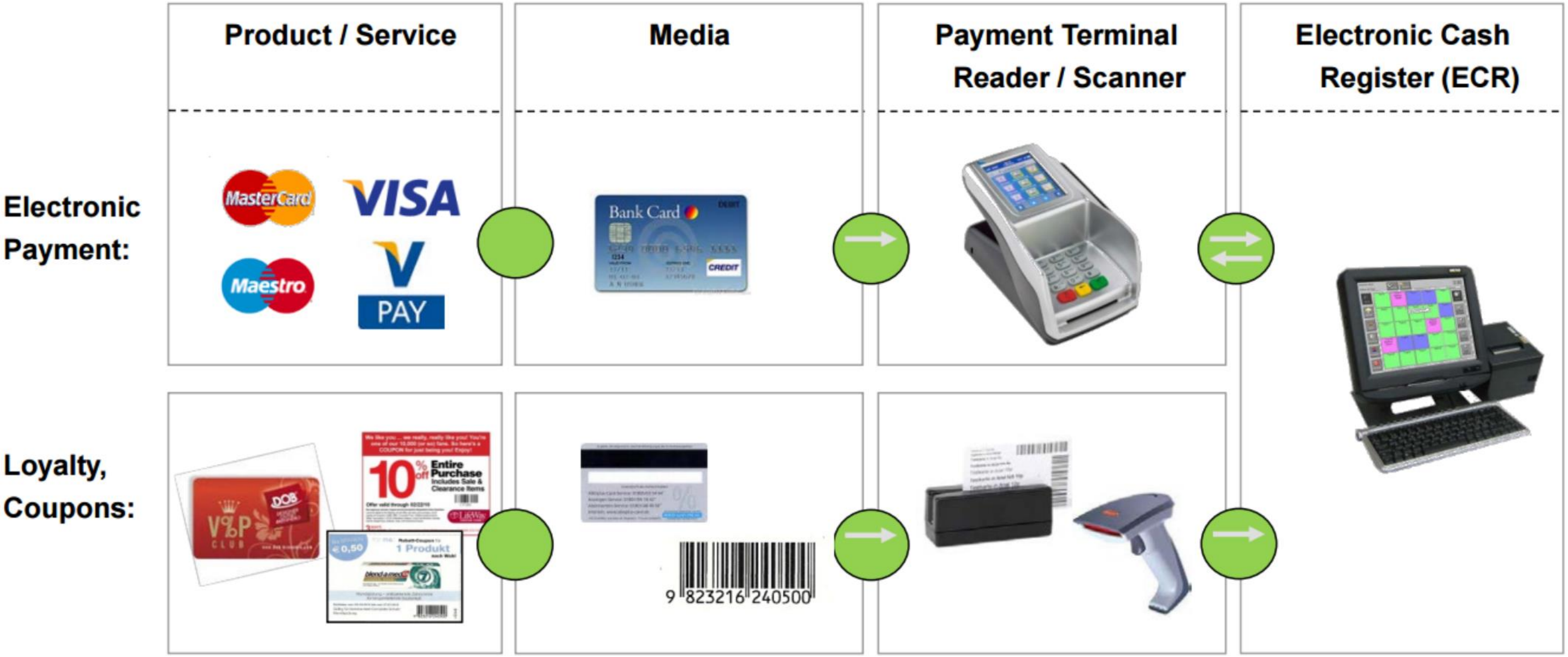
- Transaction monitoring
- Identity leaks
- De-anonymisation of transactions
- Compromise of Bitcoin wallets
- Scams with fake bitcoin merchants and retailers
- Etc…

Merchants and Retailers

- DDos attacks
- Hacking
- Double spending
- Etc.

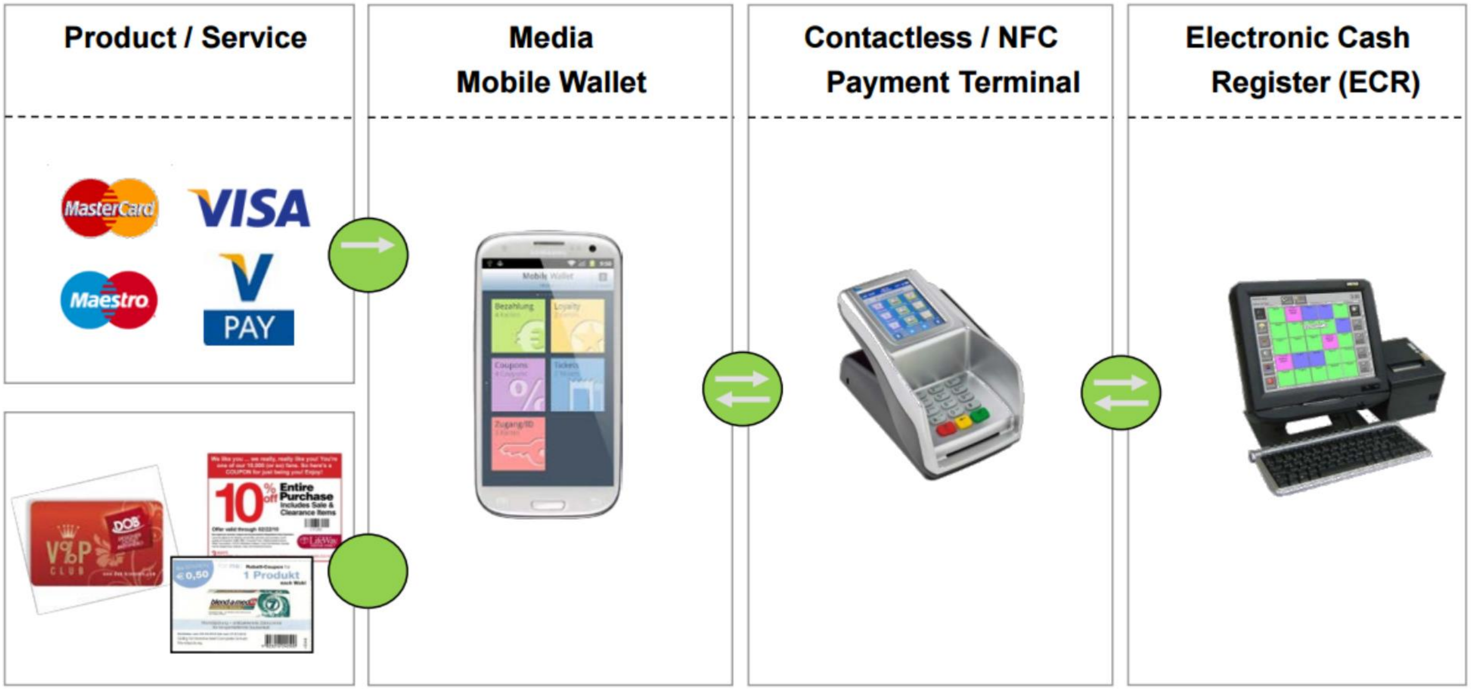
mobile business

Mobile Wallet Landscape at POS today



- Different Technology involved
- Payment and Value Added Services are managed independently from each other

Mobile Wallet
Landscape with Mobile Wallet



Electronic Payment:

Loyalty, Coupons:

Product / Service

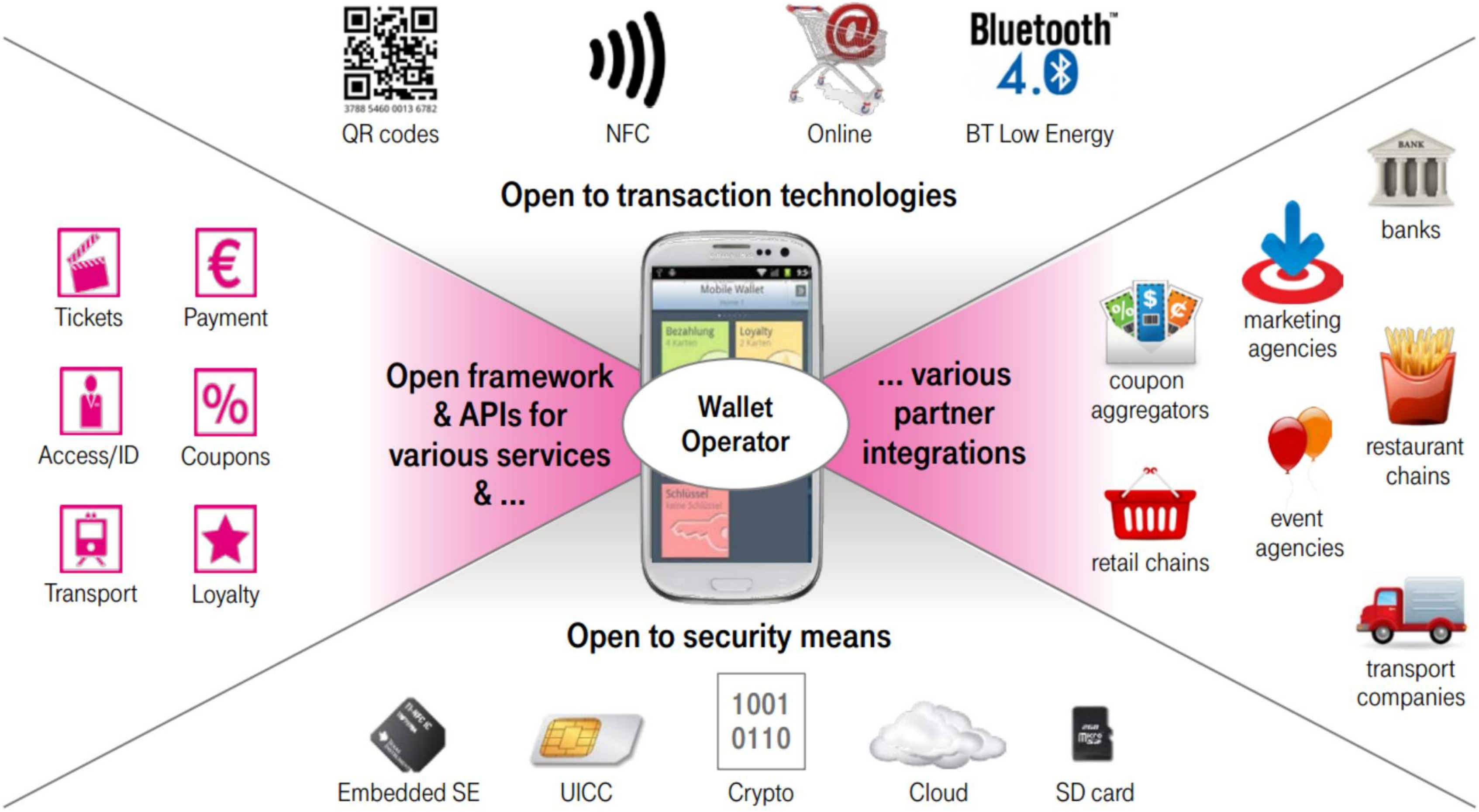
Media Mobile Wallet

Contactless / NFC Payment Terminal

Electronic Cash Register (ECR)

- Standardized interfaces between NFC device, terminal and register
- IT complexity can be improved, while NFC service is improved

Mobile Wallet
User centric Wallet as a paradigm



Topics…

- Topic 1: Bitcoin Consumer security risks
- Topic 2: Fraud scenarios and security attacks in the Bitcoin ecosystem affecting retailers and merchants
- Topic 3: Fraud scenarios in the mobile wallet ecosystem
- Topic 4: Security risks for mobile wallet consumers

Intro

PART III: IMPACT OF PRIVACY TECHNOLOGIES IN ONLINE SOCIAL NETWORKS

http://online-social-networking.com/tag/social-networking-sites

Topics…

- Topic 1: Why users participate in Online Social Networks
- Topic 2: Privacy expectations of digital natives in Online Social Networks
  - Define attitudes about online privacy focusing on OSN
- Topic 3:Potential threats to Privacy associated with the use of Online Social Networks

Topics…

- Topic 4: Workplace Privacy Policies and their capability to protect employees
- Topic 5: Privacy technologies in Online Social Networks

4. Distribution of Topics

Overview Topics

I.1	🟩	Actors involved in IP PBX fraud
I.2		Potential emerging risks of IP PBX system
I.3	🟩	Potential emerging risks of Roaming
I.4	🟩	The economic impact of roaming fraud to operators
I.5		The economic impact of roaming fraud to the subscribers
I.6		The impact of roaming fraud on the reputation of operators
I.7		Who is legally liable for damage accused by IP PBX fraud?
I.8		Requirements (considerations) of an IP PBX fraud prevention systems (approaches)
I.9		Requirements (considerations) of a Roaming fraud prevention systems (approaches)

II.1	🟩	Bitcoin Consumer security risks
II.2	🟩	Fraud scenarios and security attacks in the Bitcoin ecosystem affecting retailers and merchants
II.3	🟩	Fraud scenarios in the mobile wallet ecosystem
II.4	🟩	Security risks for mobile wallet consumers
III.1	🟩	Why users participate in Online Social Networks
III.2	🟩	Privacy expectations of digital natives in Online Social Networks
III.3	🟩	Potential threats to Privacy associated with the use of Online Social Networks
III.4	🟩	Why users participate in business realted Online Social Networks
III.5	🟩	Privacy Technologies in Online Social Networks

▨ Seminar Paper can be submitted in german

Distribution of Topics

- You will receive your "anchor" literature until start of next week (1-2 papers).
- Send 150-word abstract and first table of contents to your supervisor until May 1.
- Individual appointments possible on-request in the starting phase and in the final phase.

5. Scientific Working

Scientific Working (1)

- Based on the structure of common scientific papers (conference papers, journal articles, etc.):
  - Problem statement / Motivation / Introduction
  - State of research / Related work
  - Own contribution / Methodology
  - Summary / Conclusion / Future work
- Other formal requirements:
  - Table of contents / Structuring
  - Standardized reference list
  - Table of figures / tables

Scientific Working (2)

- Style:
  - No colloquial language
  - Be precise
  - Grammar and typo check
  - No headwords, write line of thought fully out
- References:
  - Any direct or indirect passages taken from other publications HAVE to be precisely referenced (according to the citation style of WIRTSCHAFTSINFORMATIK or MISQ)
  - Same for figures and tables, etc.
  - Avoid foot notes

Scientific Working (3)

- Literature Research:
  - Work with scientific publications
  - Avoid articles from Wikipedia and/or popular literature
  - Include the state of the art
  - Use databases for scientific literature (Google Scholar, ACM, JSTOR, citeseer, Web of Knowledge, AISNET.)

Scientific Working (4)

- Literature Management tools help with the organization of used literature.
- Mendeley:
  - Online/Offline synchronization
  - File organizer
  - One-click import
  - Word Plug-in
  - BibTex export
  - Sharing through Social Networking
  - Support of many citation styles
  - Client for Windows and Mac
  - It`s free (up to 2 GB)
  - http://www.mendeley.com/

Important Dates

Time	Where/How	
14.04.15, 10:00-12:00	2.202 (RuW)	Introduction & Assignment of Topics
01.05.15, 23:59	e-mail	Abstract & TOC
01.06.15, 23:59	e-mail	Draft version seminar paper
08.06.15, 15:00	2.257 (RuW) + e-mail	Final version seminar paper
18.06.15, 23:59	e-mail	Final version presentation
25.06.14, 09:00-18:00	2.202 (RuW)	Presentations (Day 1)*
26.06.14, 09:00-18:00	2.202 (RuW)	Presentations (Day 2)*

7. Your Questions

Literature

1. Keromytis, Angelos D. "A comprehensive survey of voice over IP security research." *Communications Surveys & Tutorials, IEEE* 14.2 (2012): 514-537. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5742777&abstractAccess=no&userType=inst
2. Rezac, Filip, and Miroslav Voznak. "Security risks in IP telephony." *Advances in Electrical and Electronic Engineering* 8.1 (2011): 15-23. http://advances.uniza.sk/index.php/AEEE/article/view/12
3. Macia-Fernandez, Gabriel, Pedro Garcia-Teodoro, and Jesus Diaz-Verdejo. "Fraud in roaming scenarios: an overview." *IEEE Wireless Communications*16.6 (2009): 88. http://www.researchgate.net/profile/Jesus_Diaz-Verdejo/publication/224093590_Fraud_in_roaming_scenarios_an_overview/links/0deec528c816a9c13a000000.pdf
4. D. Richard. Kuhn, National Institute of Standards, and Technology (U.S.). PBX vulnerability analysis: finding holes in your PBX before someone else does [Washington, D.C, 2001] http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

References

- [1] N. By, “G LOBAL T ELECOM F RAUD I NCREASES BY 0 . 21 % FROM 2011 , S TILL N EAR 5-Y EAR L OW COMMUNICATIONS FRAUD CONTROL ASSOCIATION (CFCA),” pp. 0–1, 2013.
- [2], Macia-Fernandez, G., Garcia-Teodoro, P., & Diaz-Verdejo, J. (2009). Fraud in roaming scenarios: an overview. IEEE Wireless Communications, 16(6), 88.
- [3], Nick Pantlin, European national news, (2014)

Back up topics

- Topic A: Risk prevention mechanisms for IP PBX fraud
  - Review the fraud prevention techniques of IP PBX fraud
- Topic B: Risk prevention mechanisms for roaming fraud
  - Review the fraud prevention techniques of roaming fraud
- Topic C: Investigation of fraud detection and prevention techniques for IP PBX fraud
  - show the difference between IP PBX fraud detection and prevention from economic perspective
- Topic D: Investigation of fraud detection and prevention techniques for IP PBX fraud
  - show the difference between roaming fraud detection and prevention from economic perspective

BACKUP

Telecommunication fraud

- Different type and methods of fraud

- Top four type of fraud:
  - Roaming fraud
  - Wholesale fraud
  - Premium Rate Service
  - Hardware reselling

- Methods of fraud:
  - Subscription fraud
  - PBX hacking
  - Account takeover
  - VoIP hacking
  - Dealer fraud

PBX fraud…

- Dial through
  - For both traditional and IP PBX, finding the PBX number
- Attacks on the end point control
  - E.g. attack through the web interface of the end points
- Attacks to PBX admin portal
  - When the attacker got the administration portal, all the controls on PBX will be disclosed.
  - Automatic call generation or dial through could happen
- Misconfiguration of the PBX