Information & Communication Security (SS 2016)

Introduction

Dr. Jetzabel Serna-Olvera
@sernaolverajm
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

Prof. Dr. Kai Rannenberg
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

mobile business

Who we are

Business Informatics @ Goethe University Frankfurt

E-Finance Prof. Dr. Peter Gomber	**Business Informatics (Informatics)** Prof. Dr. Mirjam Minor	**Information Systems Engineering** Prof. Dr. Roland Holten
Business Education (associated) Prof. Dr. Gerhard Minnameier	**Business Informatics**	**Business Education** (associated) Prof. Dr. Eveline Wuttke
Information Systems & Information Management Prof. Dr. Wolfgang König	**Business Informatics & Microeconomics** Prof. Dr. Lukas Wiewiorra	**Mobile Business & Multilateral Security** Prof. Dr. Kai Rannenberg

Chair

Chair of Business Administration, especially Business Informatics, Mobile Business and Multilateral Security

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Theodor-W.-Adorno-Platz 4
Campus Westend
RuW, 2nd Floor

Phone:	+49 69 798 34701
Fax:	+49 69 798 35004
e-mail:	info@m-chair.de

www.m-chair.de

Team

Kai Rannenberg

Jetzabel Serna-Olvera

Sebastian Pape

Shuzhe Yang

David Harborth

Fatbardh Veseli

Christopher Schmitz

Welderufael Tesfay

Ahmed S. Yesuf

Research Fellows & External PhD Students

Gökhan Bal

Mike Radmacher

Andreas Albers

Stefan Weiss

Christian Kahl

André Deuker

Markus Tschersich

Sascha Koschinat

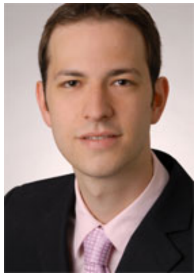
Stephan Heim

Lars Wolos

Tim Schiller

Niels Johannsen

Ahmad Sabouri


Marvin Hegen

Team

Office:

Elvira Koch

Email: elvira.koch@m-chair.de

Office Hours: Mo.-Fr. 10:00-14:00

Kai Rannenberg

Vita of Kai Rannenberg

Einbeck, Göttingen, Eystrup, Wolfsburg, ...
TU Berlin (Dipl.-Inform.)
Uni Freiburg (Dr. rer. pol.)

Dissertation "**Kriterien und Zertifizierung mehrseitiger IT-Sicherheit**"
Standardization at ISO/IEC JTC 1/SC 27 and DIN NI-27

Kolleg "Sicherheit in der Kommunikationstechnik"
Gottlieb Daimler- and Karl Benz-Foundation

Multilateral Security:
"Empowering Users, Enabling Applications", 1993 - 1999

Recent history of Kai Rannenberg

1999-09 till 2002-08

Microsoft Research Cambridge UK

www.research.microsoft.com

Responsible for “Personal Security Devices and Privacy Technologies“

2001-10 Call for this chair

2001-12 till 2002-07 Stand-in for the chair

Since 2002-07 Professor

Dr. Jetzabel Serna-Olvera

Assistant Professor

Short-bio

- 1997-2001 - “Instituto Tecnológico de Tijuana” (Tijuana) – Computer Systems Engineering
- 2003-2006 – “Gerhard Mercator Universität” (Duisburg-Essen) – Master of Science in Computer Science and Communications Engineering
- 2006-2008 – “Universität Politècnica de Catalunya” (Barcelona) – Diploma of Advanced Studies
- 2008-2012 – “Universität Politècnica de Catalunya” (Barcelona) – PhD in Computer Architecture and Technology

- 2001-2002 - H. Ayuntamiento de Tijuana (Tijuana) – Software Developer
- 2005-2006 - CoCoNet AG (Erkrath) – Software Developer
- 2006-2011 – Escert-UPC (Barcelona) – Security Researcher
- 2011-2014 – Barcelona Digital Technology Centre (Barcelona) – Security Intelligence Senior Researcher

Research Focus

- Security, Privacy and Trust in Distributed Environments

mobile business

Dr. Jetzabel Serna-Olvera

Projects

Security

Smart Cybercrime Data Collection and Exchange
+
Mobile Banking Security

COIM-best

Coordination improvement by best practices

integra

Research in Migration Management Technologies

Identity Management

enisa
European Network and Information Security Agency

electronic IDentity and Authentication Systems (eIDAS) used in e-Finance Services

SEGURIDAD 2020

Identity Management in Digital Territories

FIDELITY
Federated Identity Management based on LIBERTY

Federated Identity Management based on Liberty

Social Networks

social media

Methods and Technologies for Social Media

CIUDAD 2020

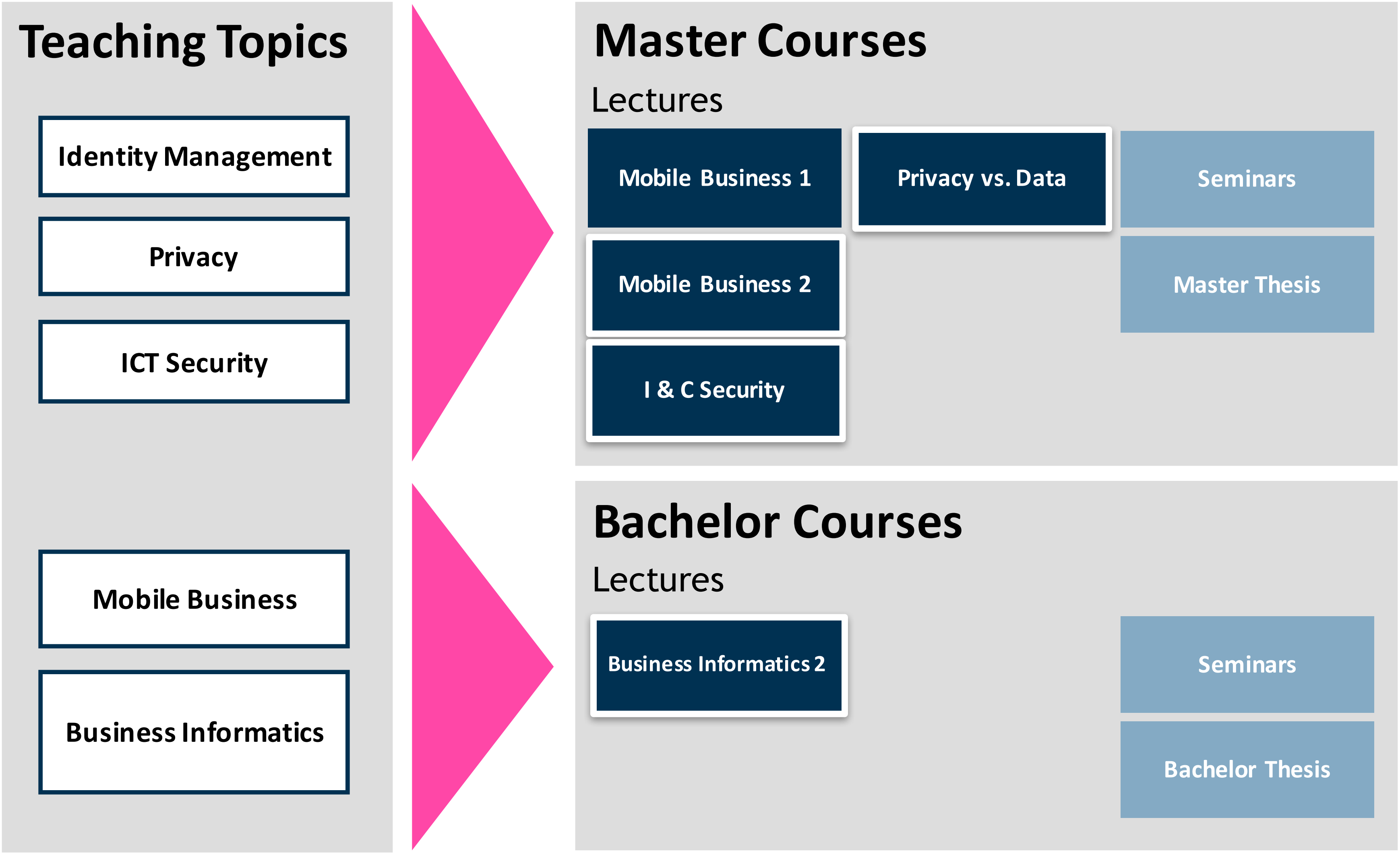
Towards a new sustainable Smart City model

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

mobile business

Teaching in Frankfurt



Teaching Topics

Identity Management

Privacy

ICT Security

Mobile Business

Business Informatics

Master Courses

Lectures

Mobile Business 1

Privacy vs. Data

Seminars

Mobile Business 2

Master Thesis

I & C Security

Bachelor Courses

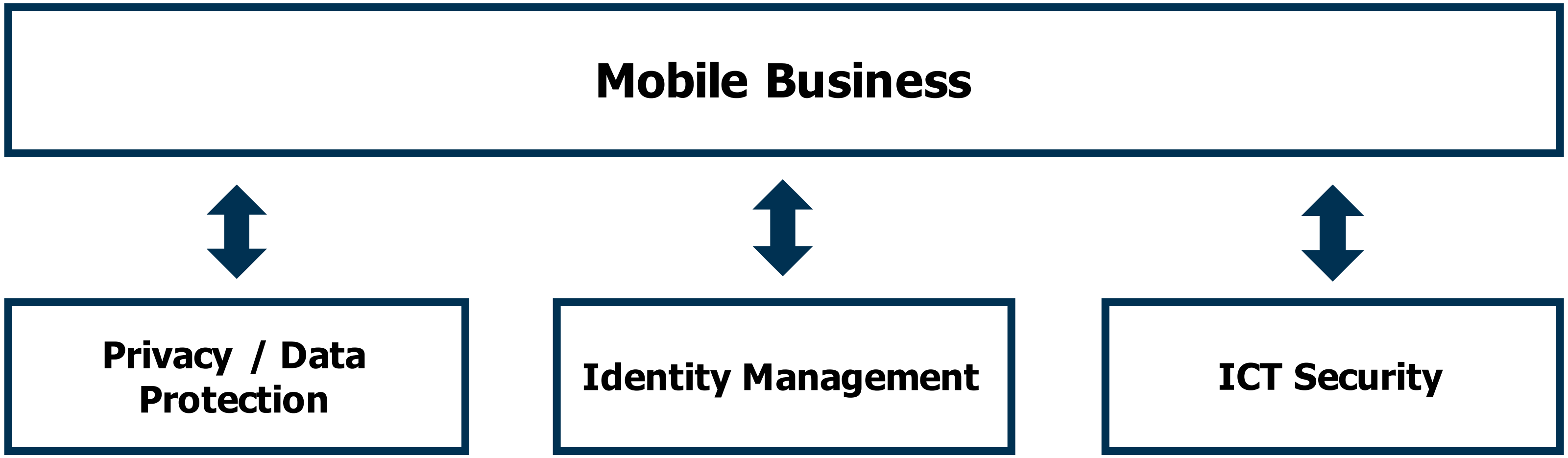
Lectures

Business Informatics 2

Seminars

Bachelor Thesis

M-Chair Research Statement



Mobile Business

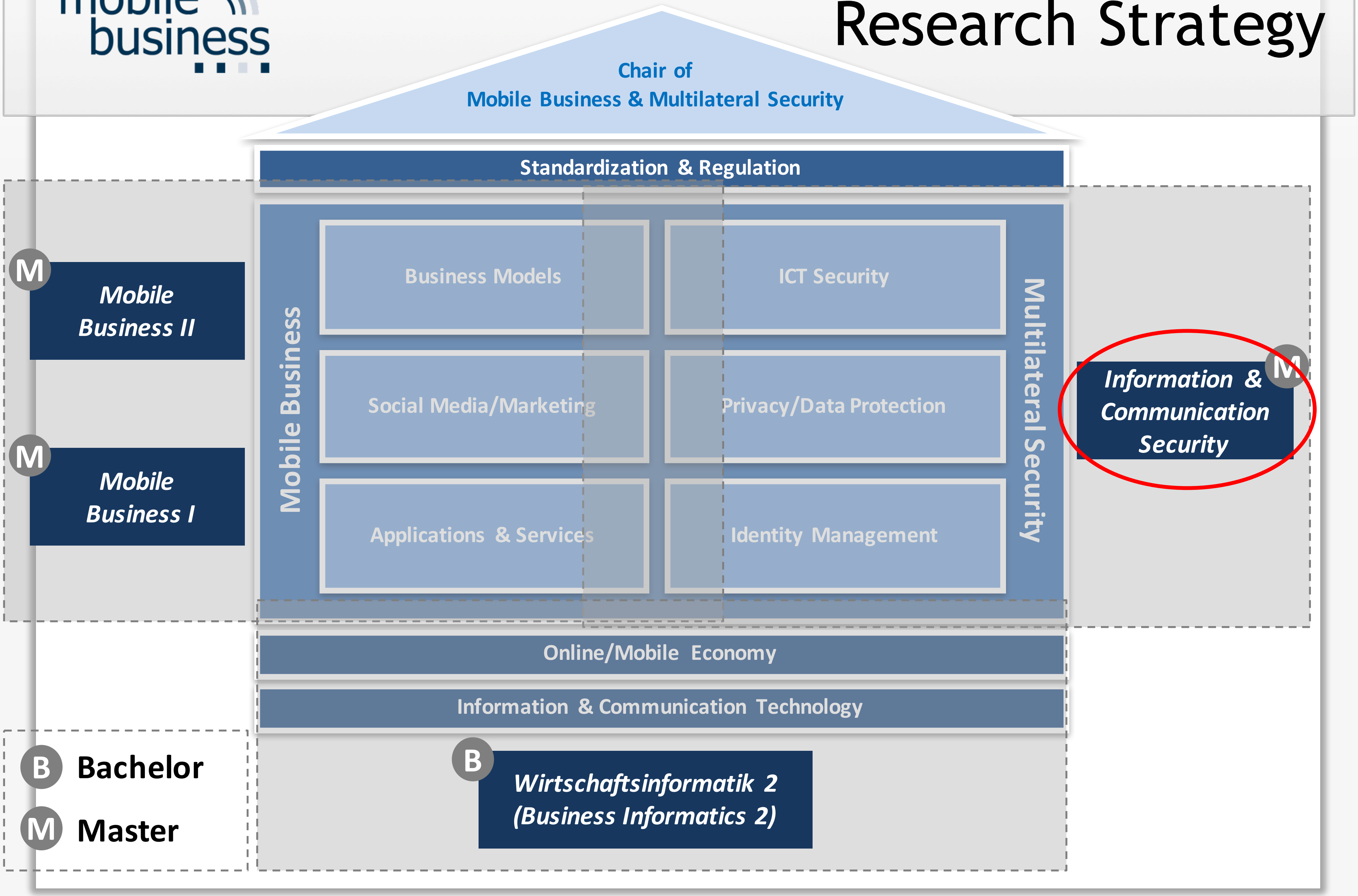
Privacy / Data Protection

Identity Management

ICT Security

Advancing ***Mobile Business*** while enabling individuals to be in control of their personal data by providing ***Identity Management***, ***Privacy Protection***, and ***ICT Security*** within the Digital Economy

Teaching & Research Strategy



Chair of
Mobile Business & Multilateral Security

Standardization & Regulation

Mobile Business

Business Models

Social Media/Marketing

Applications & Services

ICT Security

Privacy/Data Protection

Identity Management

Multilateral Security

Online/Mobile Economy

Information & Communication Technology

M *Mobile Business II*

M *Mobile Business I*

M *Information & Communication Security*

B *Wirtschaftsinformatik 2 (Business Informatics 2)*

B Bachelor

M Master

mobile business

M-Research in Frankfurt

- Multilateral Security
  - Security, Trust, Identity Management, and Privacy
  - Mobile Signatures
  - Personal Security Devices
- Mobile Life, Work, and Business
  - Location-based Services
  - Mobile Communities
- M-Infrastructures
  - Combination, Integration, Innovation
  - Standardization, Regulation

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

INKO - Contact Persons

M.Sc. Ahmed S. Yesuf

RuW Building, Office 2.236

Phone: 069 / 798 – 34699

Email: ahmed.yesuf@m-chair.de

M.Sc. Welderufael B. Tesfay

RuW Building, Office 2.235

Phone: 069 / 798 – 34706

Email: welderufael.tesfay@m-chair.de

Followme! twitter.com/mchair

sec@m-chair.de

Ahmed S. Yesuf

Research Assistant

General Research Interests:

- Risk modelling and analysis approaches
- Secure software development
- Design and requirement engineering
- Usability of Risk Assessment techniques

PhD focus

- Risk assessment of Socio-technical systems specifically to the telecommunication services

Projects:

- TRE$_{s}$PASS (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security)

Welderufael Tesfay

Research Assistant

Research Interests:

- Mobile and Pervasive Computing
- Open Source Mobile Platforms, Applications and Services
- Human Factors of Security and Privacy
- Applied Cryptography and Smart Cards

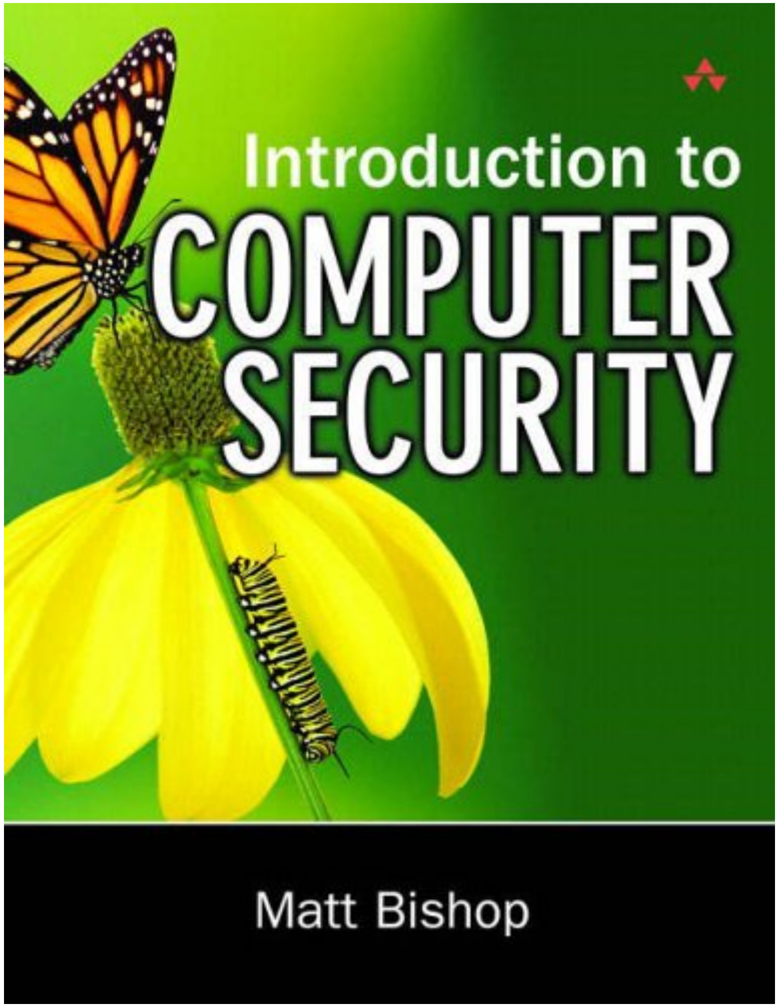
PhD Focus:

- Usable Privacy Enhancing Technologies with Focus on Privacy-ABCs
- Learning from User Data to Enhance User Privacy

Projects:

- CREDENTIAL

Literature



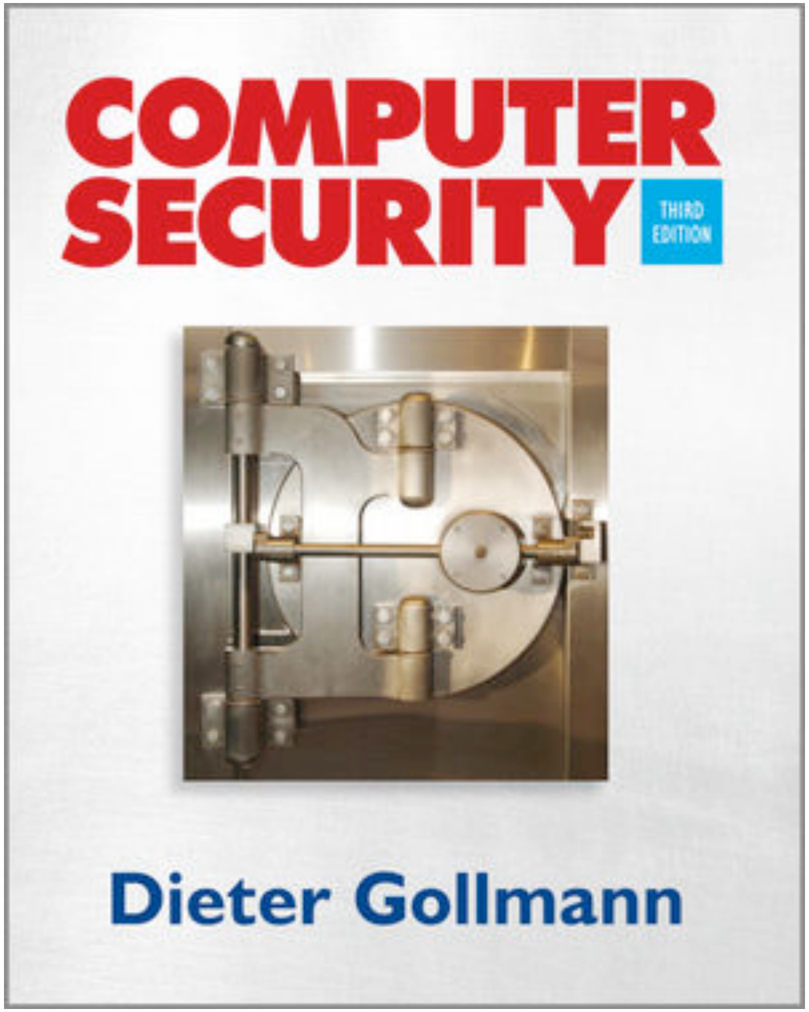
Matt Bishop:

Introduction to
Computer Security

Addison Wesley

ISBN: 0-321-24744-2

Literature



Dieter Gollmann:

Computer Security

John Wiley & Sons

ISBN: 0-470-74115-5

Literature

Oldenbourg Verlag

Claudia Eckert

IT-Sicherheit

Konzepte – Verfahren – Protokolle

7. Auflage

In German:

Claudia Eckert:

IT-Sicherheit

Oldenbourg

ISBN: 978-3-486-70687-1

Literature

Please Note:

Electronic library of Journals, access to more than 2000 Journals

http://www.ub.uni-frankfurt.de/online/emedien.html

Available only for University members via HRZ account (141.2.XXX.XXX IP-addresses; PC Pool) or via University Library login:
www.ub.uni-frankfurt.de/login.html

JSTOR

search.epnet.com/login.asp
www.jstor.org

EBSCO HOST Research Databases

Online search engines:

scholar.google.com
academic.live.com

On the dates and the agenda

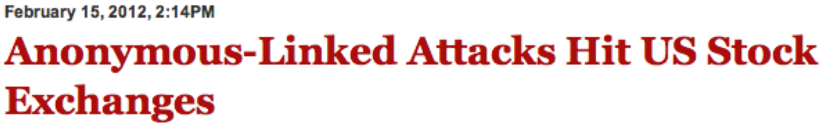
- **Exam date not fixed yet.**
  - Please keep yourself updated!
  - Check the website of the Prüfungsamt: http://www.wiwi.uni-frankfurt.de/mein-wiwi-studium/pruefungsamt.html
- **Course agenda is online.**
  - Please keep yourself updated!
  - Check the website of the course: https://m-chair.de/index.php?option=com_teaching&view=lecture&id=21

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

mobile business

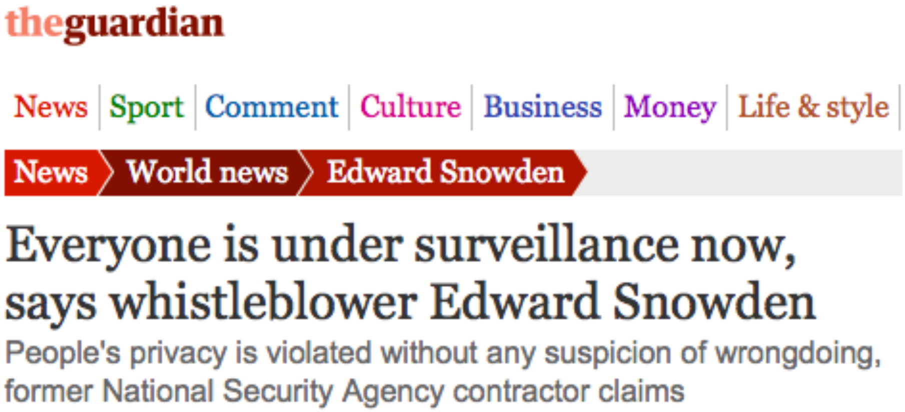
Electronic Business and Security



February 15, 2012, 2:14PM

Anonymous-Linked Attacks Hit US Stock Exchanges

(Distributed) „Denial of Service“-Attacks on e-auctioneers/broker/betting office

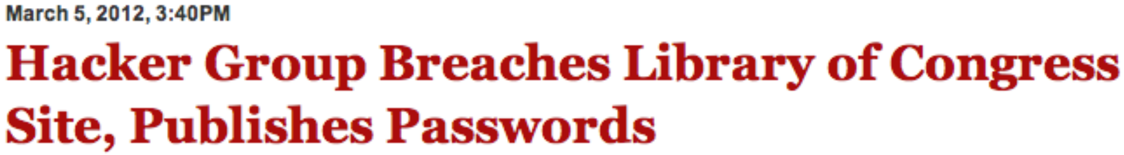


theguardian

News | Sport | Comment | Culture | Business | Money | Life & style
News > World news > Edward Snowden

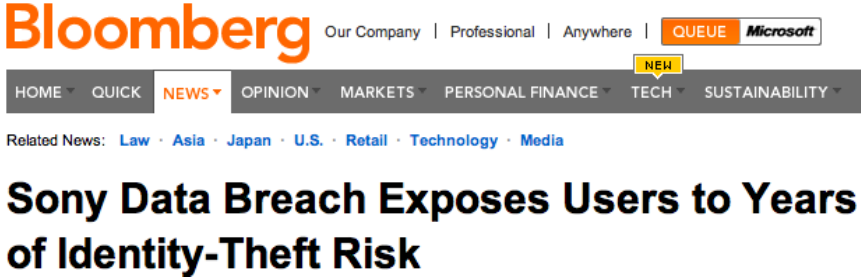
Everyone is under surveillance now, says whistleblower Edward Snowden

People's privacy is violated without any suspicion of wrongdoing, former National Security Agency contractor claims



March 5, 2012, 3:40PM

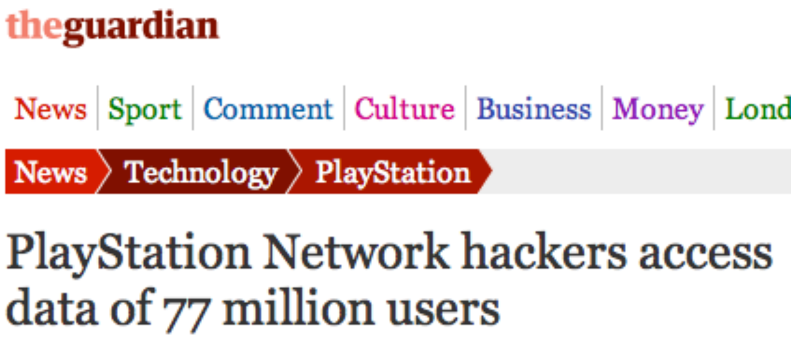
Hacker Group Breaches Library of Congress Site, Publishes Passwords



Bloomberg

Our Company | Professional | Anywhere | QUEUE Microsoft
HOME QUICK NEWS OPINION MARKETS PERSONAL FINANCE NEW TECH SUSTAINABILITY
Related News: Law · Asia · Japan · U.S. · Retail · Technology · Media

Sony Data Breach Exposes Users to Years of Identity-Theft Risk



theguardian

News | Sport | Comment | Culture | Business | Money | Lond
News > Technology > PlayStation

PlayStation Network hackers access data of 77 million users

Risks of Unprotected Market Activities

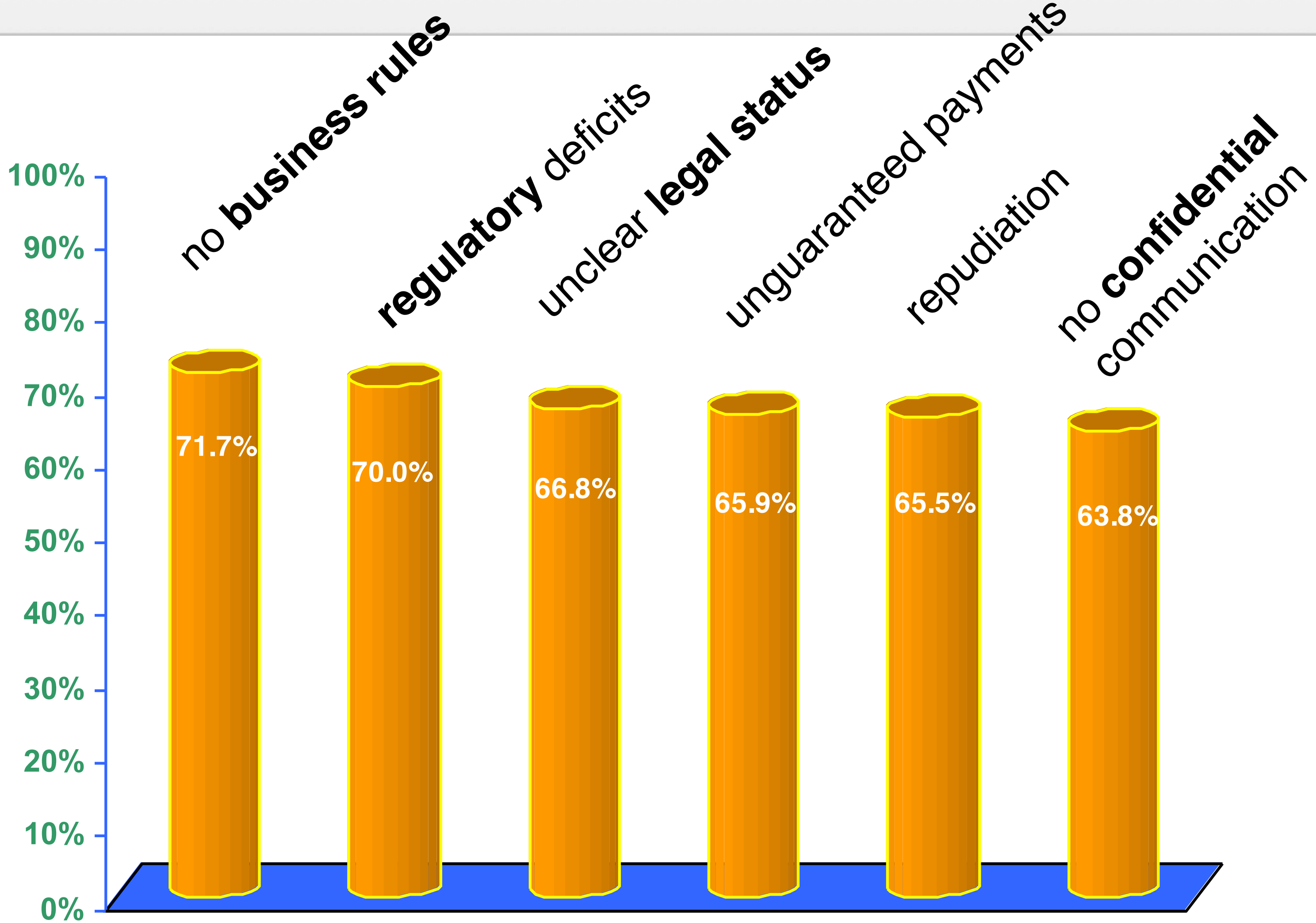
Provider

- no payment – debtor cannot be captured
- wrong or fake orders
- copyright violations
- www attacks
- internal server intrusion
- …

Consumer

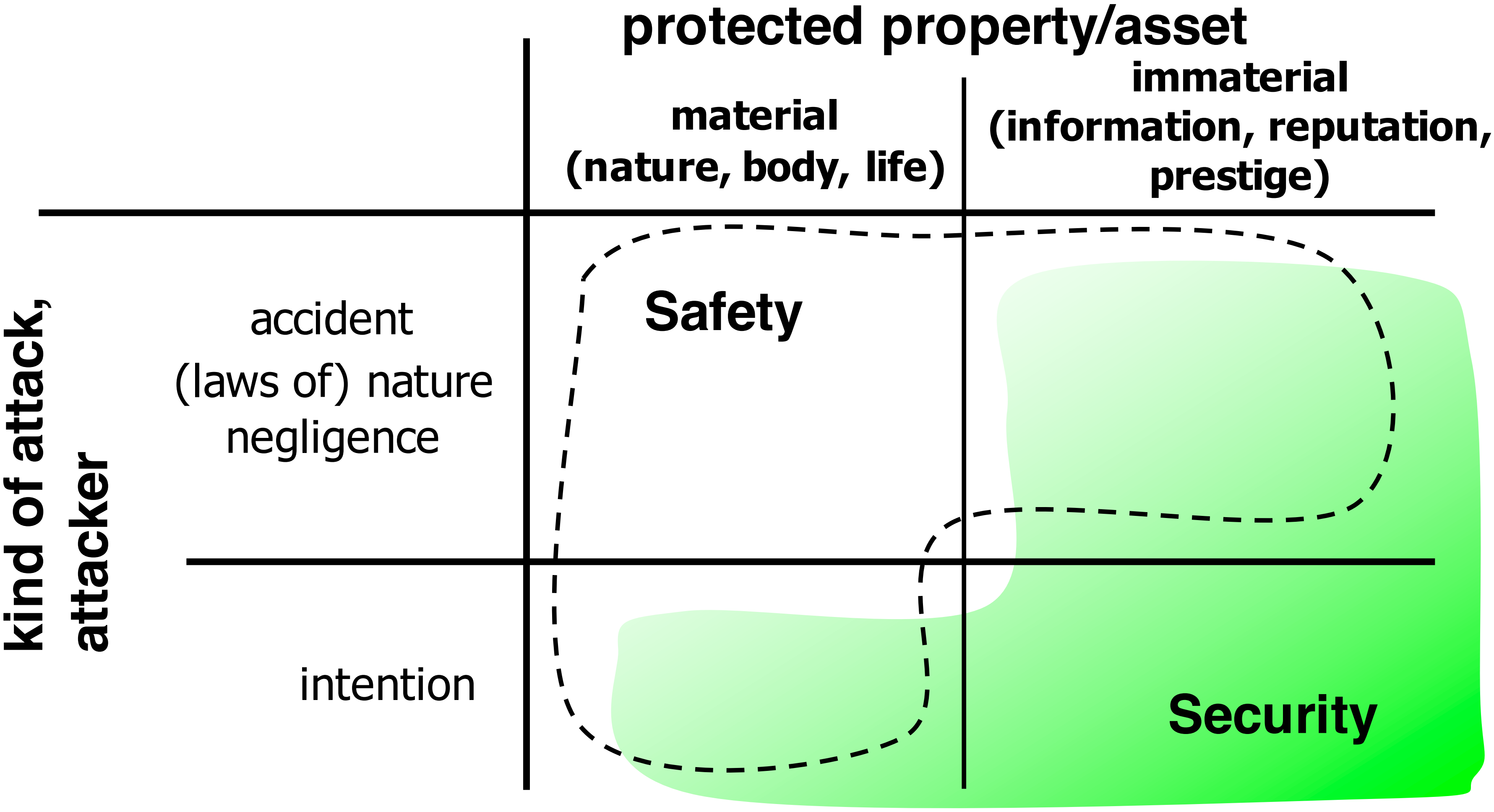
- unwanted deliveries (false, not ordered, …)
- unauthorized / unexpected direct debt of money, e.g. from a credit card account
- unwanted advertising mail (“spamming”)
- transparent consumers
- …

E-Commerce Requires Security



Source: Electronic Commerce Enquête, Universität Freiburg, 1998
(32 options + free text for choice, 6 options with highest agreement listed)

Security vs. Safety



protected property/asset

material (nature, body, life)

immaterial (information, reputation, prestige)

kind of attack, attacker

accident
(laws of) nature
negligence

intention

Safety

Security

Security

A very human discrepancy

- **Privacy**

  Protect the own sphere and the own values/assets
- **Binding**

  Gain trust (of partners), transfer values

Kind of technical arrangement

- **Confidentiality**
  Information delivery just to whom it is intended
- **Integrity**
  no faking of information
- **Availability**
  no system failures / no loss of data
- **Accountability**
  actions are always accountable to responsible parties

A **combination** of technical, organizational and legal methods is necessary.

Concepts and their Motivation (1)

- ***Unauthorized earning of information***, that means loss of **confidentiality**: patient data (for example information of physical examinations, diagnoses or therapy attempts, but also content of meetings on patient cases which is stored in databases) shall not accessible to unauthorized persons (e.g. other patients, hospital employees or employees of the network operator whose (mobile) network is used to transfer the data from hospital to hospital).

- ***Unauthorized modification*** of information, that means loss of **integrity**: Unauthorized and unobserved data modifications (e.g. a prescription, a medicament ordering or a dosage instruction) may lead to life-threatening consequences.

Concepts and their Motivation(2)

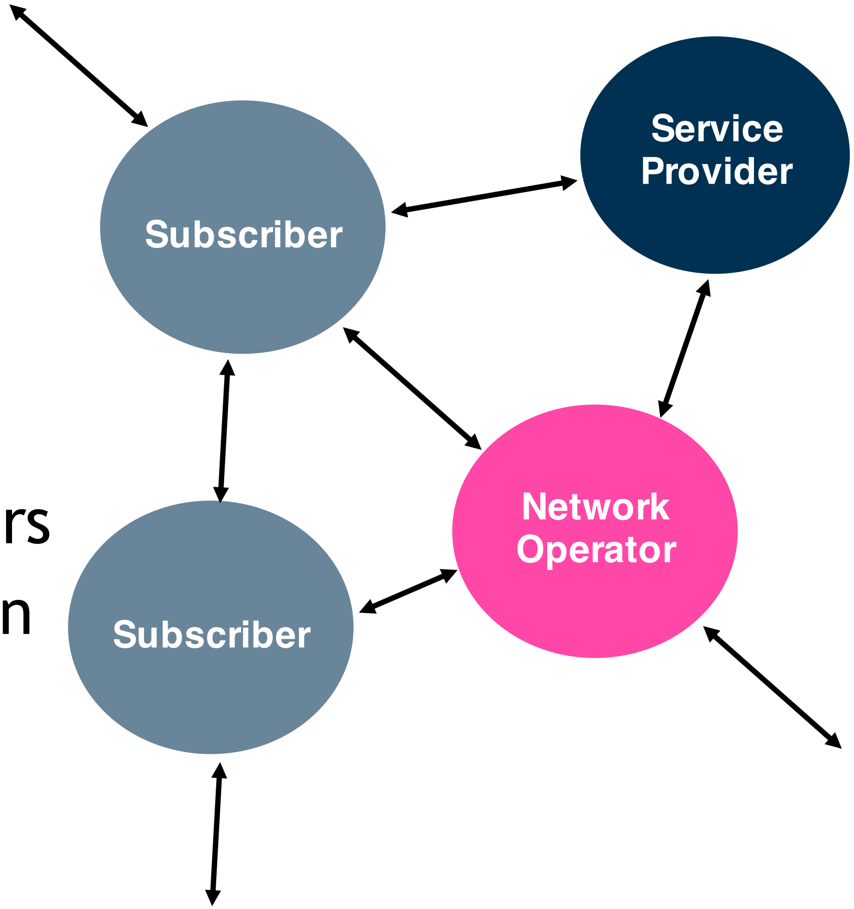
- ***Unauthorized impair of functionality***, that means loss of **availability**: If the medical history is accessible solely via one network and this network has a breakdown when patient data has to be queried it may be life-threatening for the patient.

- ***Incorrect non-committalness***, that means loss of **accountability**: If the persons liable for procedures in IT-systems (e.g. for the delivery of diagnoses, therapy instructions or billings) cannot be identified unwarrantable actions may occur. Moreover, the consequences of a mistake may be worse for the injured party since there is no information on whom to ask for compensation.

Multilateral Security

Different Parties
with
different Interests

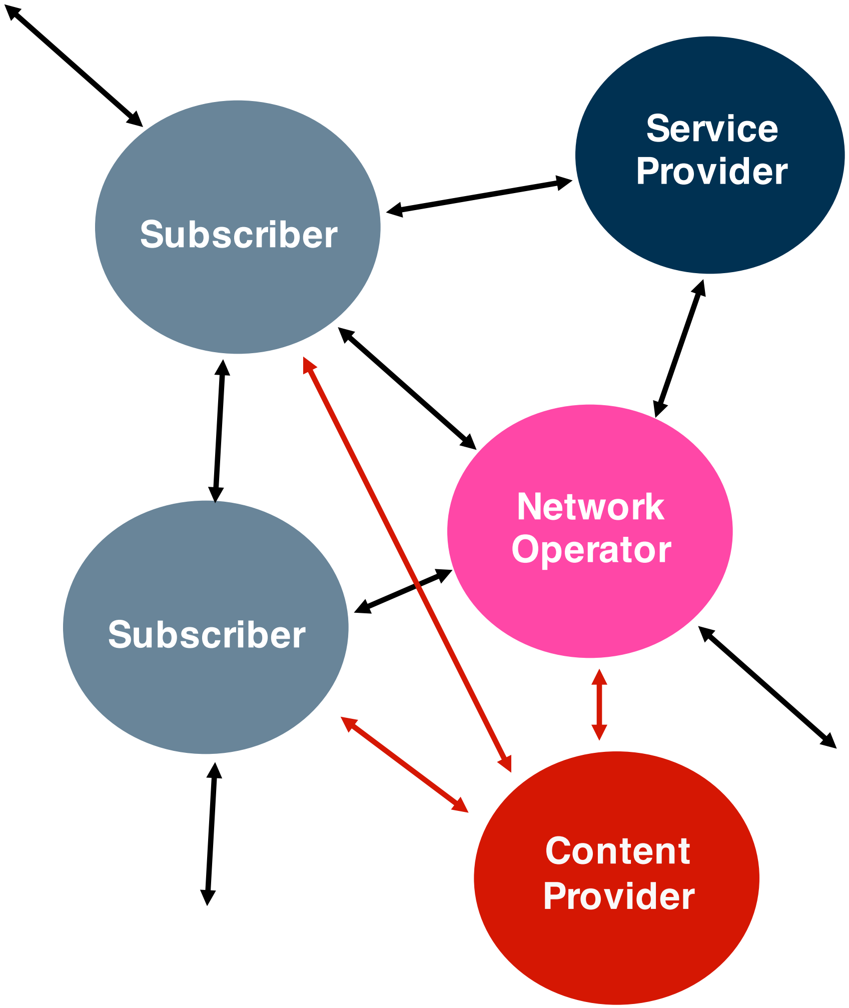
- Customers/Merchants
- Communication partners
- Citizens/Administration



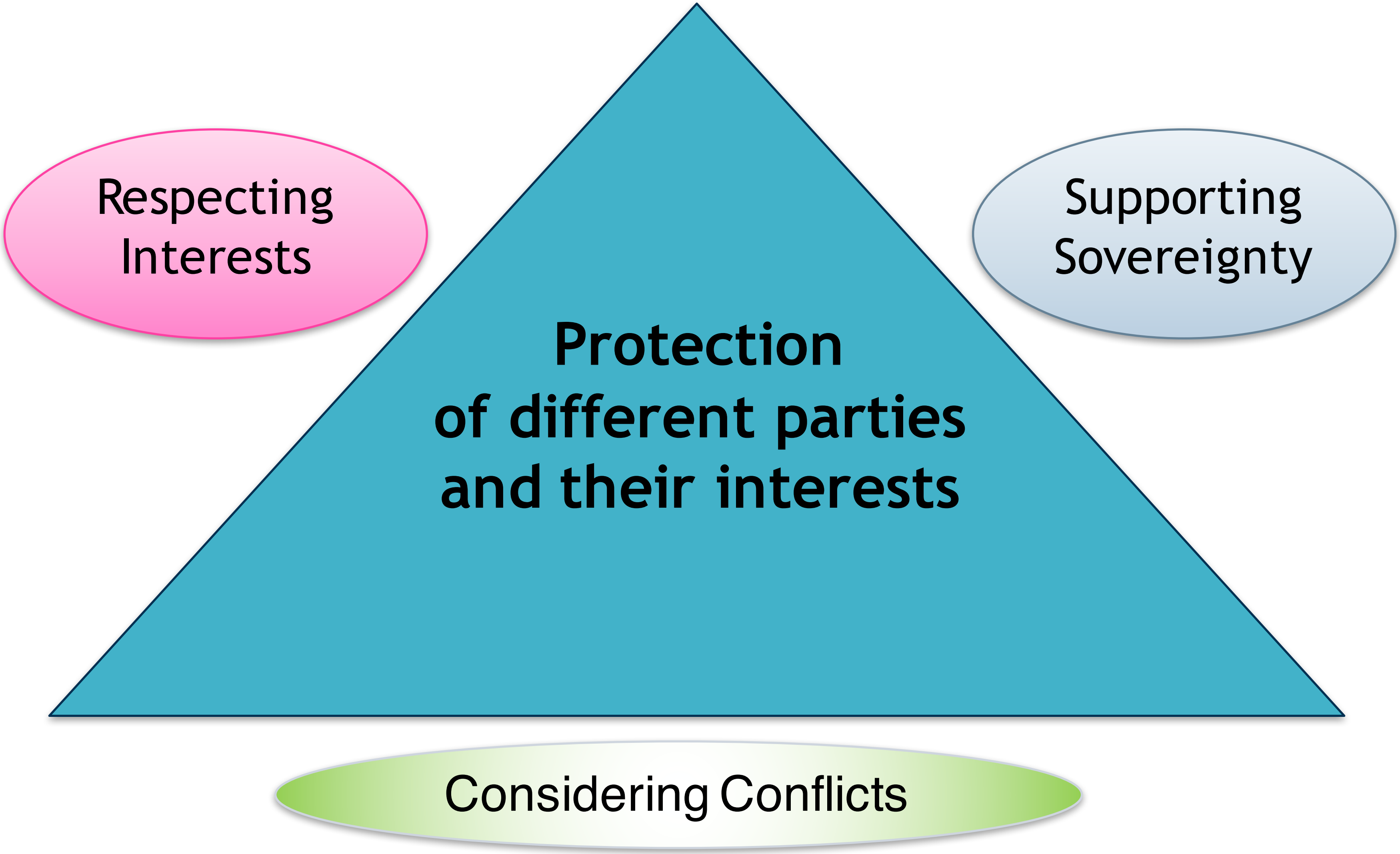
Multilateral Security

… in a world of consortia

- more partners
- more complex relations



Multilateral Security



Respecting Interests

Supporting Sovereignty

Protection of different parties and their interests

Considering Conflicts

Multilateral Security considers conflicts

Respecting Interests

- Parties can define their own **interests.**
- Conflicts can be **recognized** and **negotiated.**
- Negotiated **results** can be reliably **enforced.**

Supporting Sovereignty

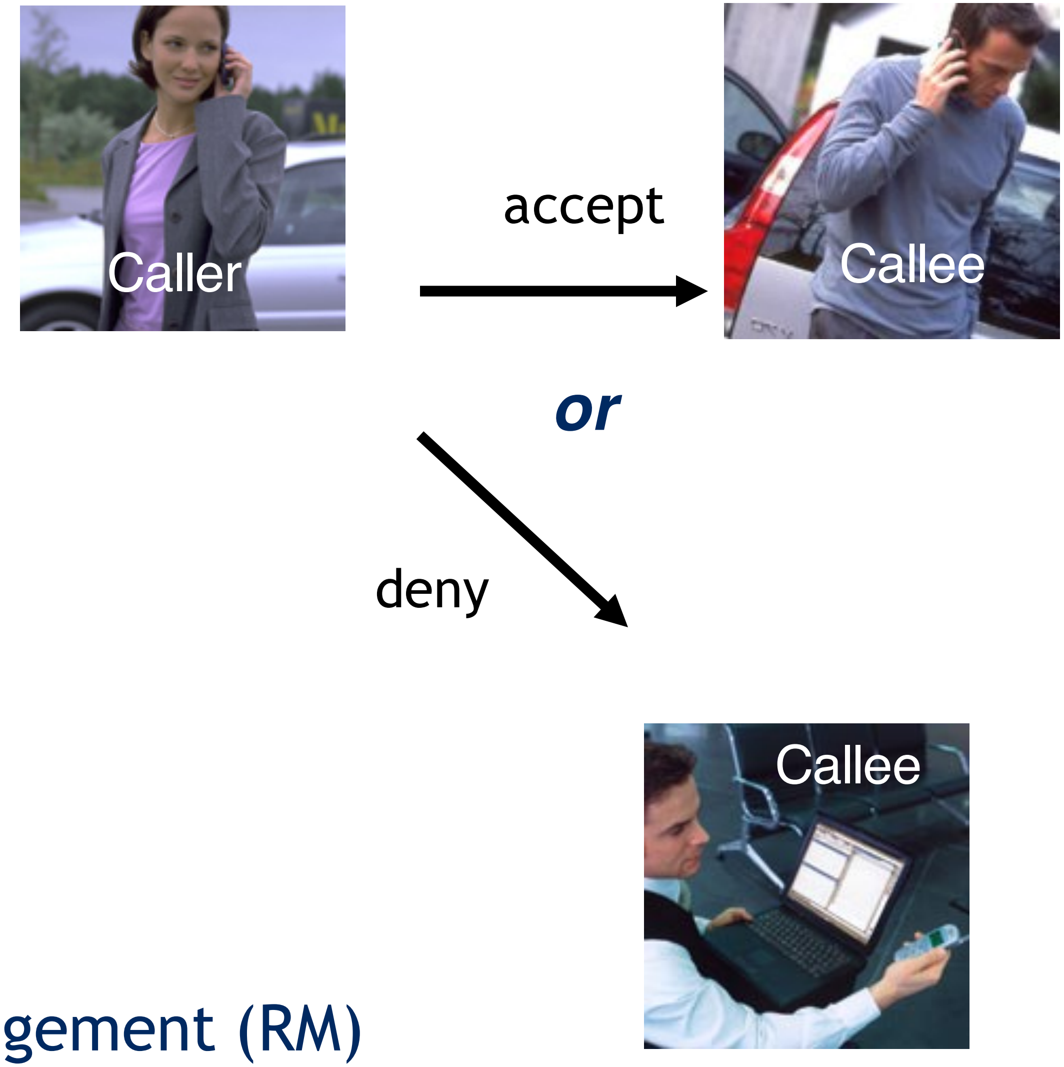
- Requiring each party to **only minimally trust** in the honesty of **others**
- Requiring **only minimal or no trust in technology** of others

Protection of **different parties** and their **interests**

Multilateral Security in daily communication

The Challenge

- Increased reachability due to new communication services
- Annoying calls
- Shortage of time
- Caller-ID conflict



accept

or

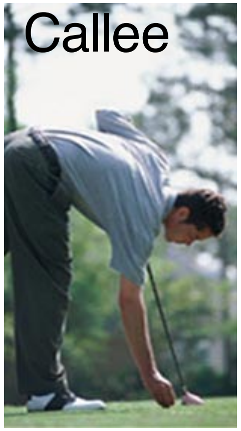
deny

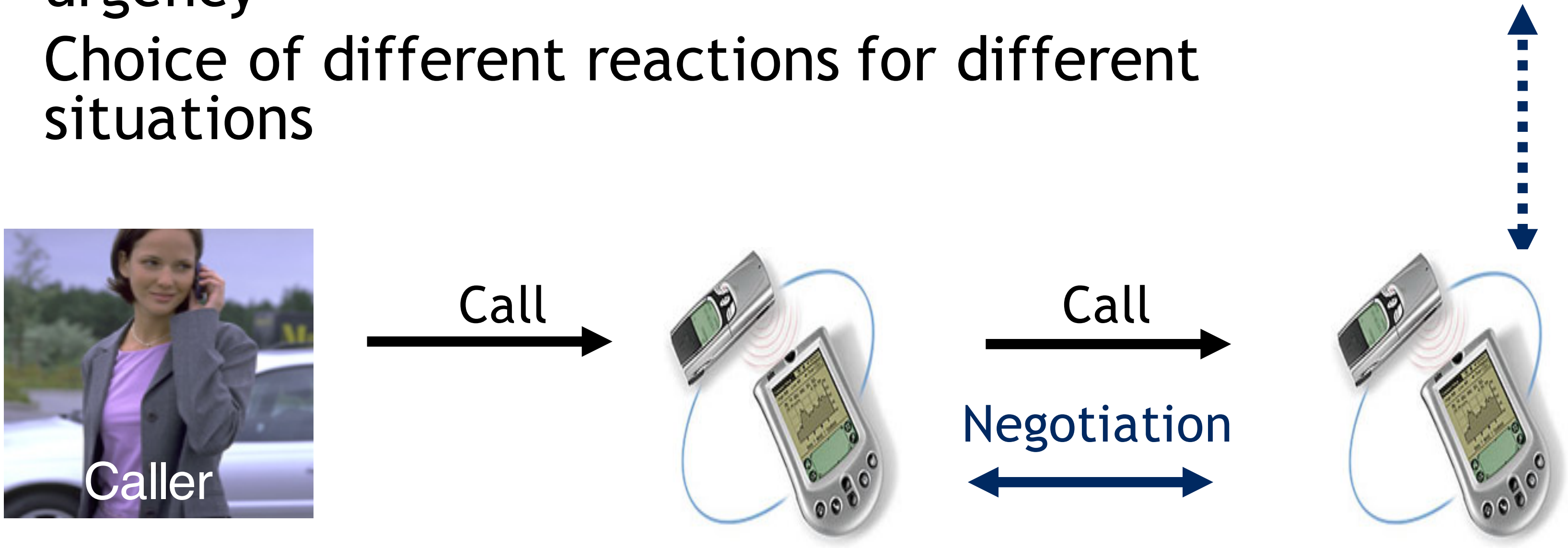
→ Reachability Management (RM)

Reachability Management

The Features

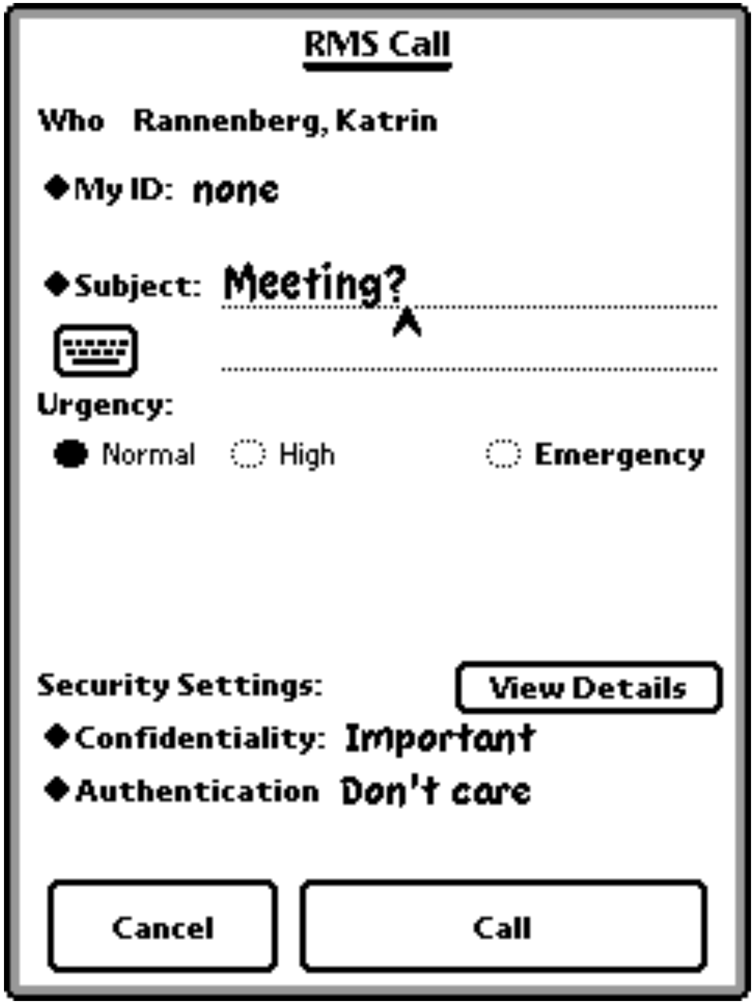
- Automatic call filtering under user control
- Privacy protection for both caller and callee
- Choice of different ways to express urgency
- Choice of different reactions for different situations





Topics of Negotiation

- Urgency of the call
- Extent of identification
- Security requirements
  - authentication
  - confidentiality
  - non-repudiation



RMS Call

Who Rannenberg, Katrin

◆My ID: none

◆Subject: Meeting?

Urgency:

● Normal ○ High ○ Emergency

Security Settings:

◆Confidentiality: Important

◆Authentication Don't care

Why should your call go through?

Statement of urgency

“It is really urgent!”

Specification of a function

“I am your boss!”

Specification of a subject

“Let’s have a party tonight.”

Presentation of a voucher

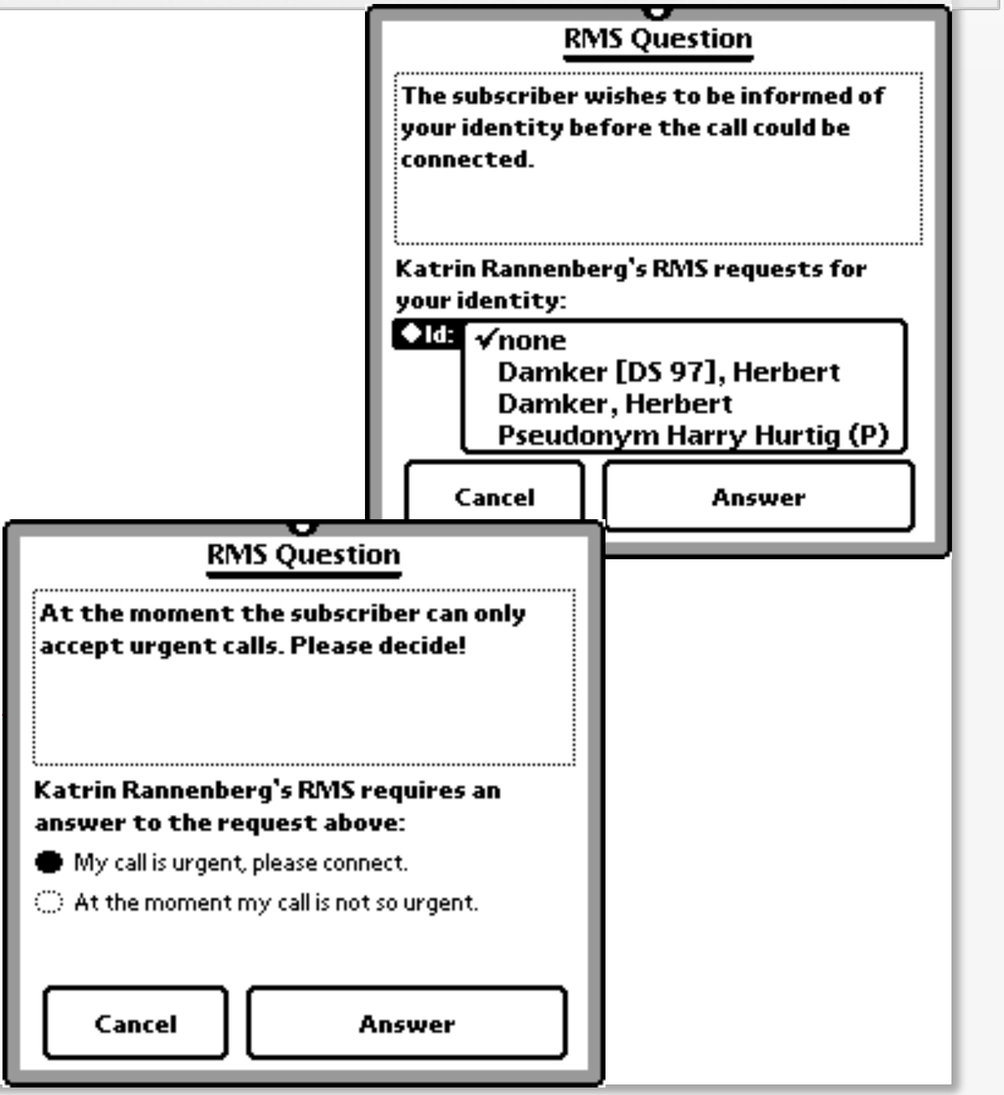
“I welcome you calling back.”

Provision of a reference

“My friends are your friends!”

Offering a surety

“Satisfaction guaranteed
or this money is yours!”



RMS Question

The subscriber wishes to be informed of your identity before the call could be connected.

Katrin Rannenberg's RMS requests for your identity:

Id: ✓none
Damker [DS 97], Herbert
Damker, Herbert
Pseudonym Harry Hurtig (P)

RMS Question

At the moment the subscriber can only accept urgent calls. Please decide!

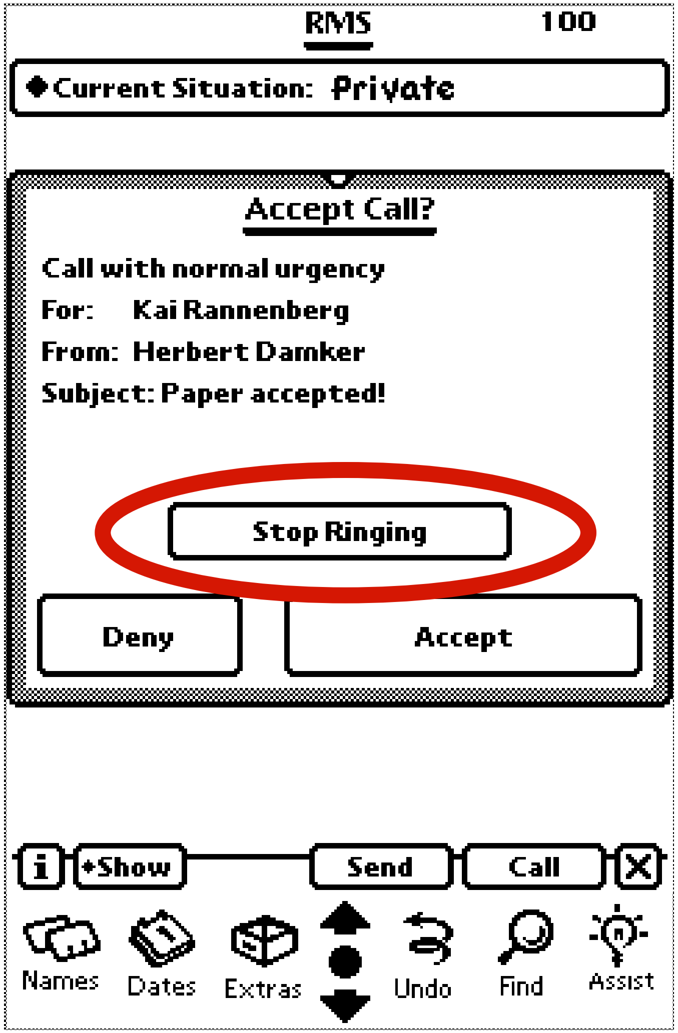
Katrin Rannenberg's RMS requires an answer to the request above:

● My call is urgent, please connect.

○ At the moment my call is not so urgent.

RMS accepted call (Callee display)

- Bell is ringing!
- Callee notified
- Callee can still decide to accept or deny the call



RMS 100

◆Current Situation: Private

Accept Call?

Call with normal urgency

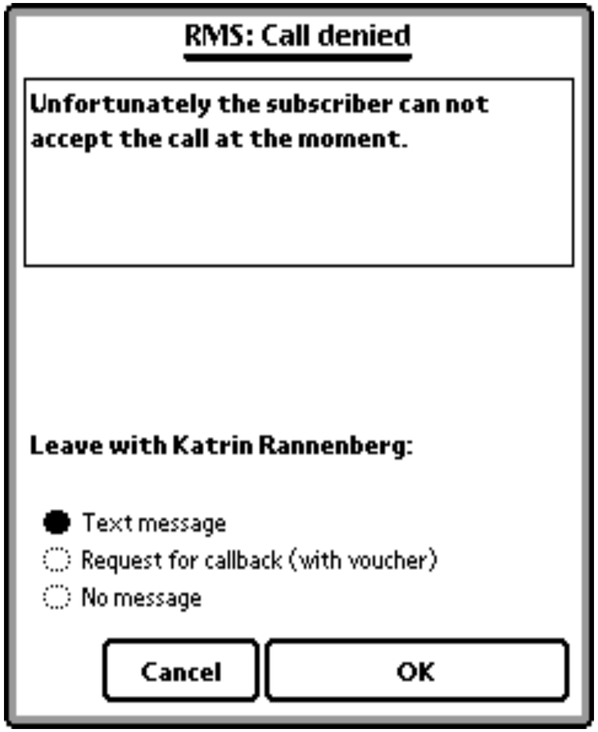
For: Kai Rannenberg

From: Herbert Damker

Subject: Paper accepted!

RMS denied call (Caller display)

- Call not connected
- Caller gets information (configured by callee)
- Caller can leave a message or request a call back



RMS: Call denied

Unfortunately the subscriber can not accept the call at the moment.

Leave with Katrin Rannenberg:

● Text message
○ Request for callback (with voucher)
○ No message

Configuring your RMS

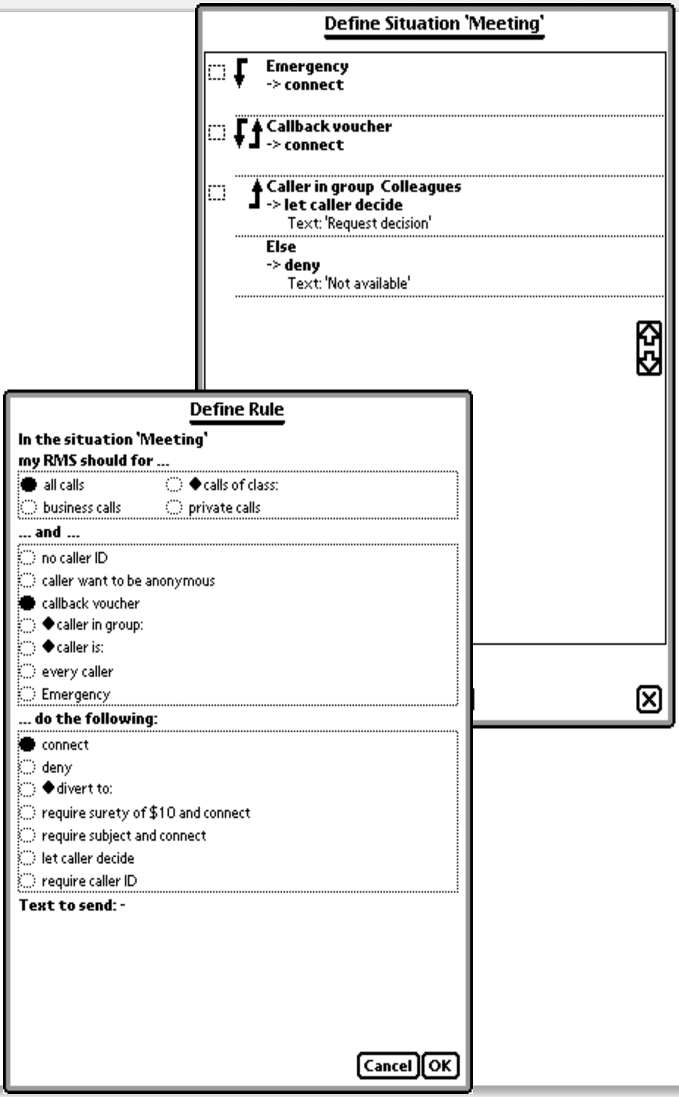
Situations

Set of rules how to deal with an incoming call

Rules

Combination of features

Users can reconfigure initial rules and situations as they like.



Define Situation 'Meeting'

□ **Emergency**
-> connect

□ **Callback voucher**
-> connect

□ **Caller in group Colleagues**
-> let caller decide
Text: 'Request decision'

Else
-> deny
Text: 'Not available'

Define Rule

In the situation 'Meeting'
my RMS should for ...

● all calls ○ ◆calls of class:
○ business calls ○ private calls

... and ...

○ no caller ID
○ caller want to be anonymous
● callback voucher
○ ◆caller in group:
○ ◆caller is:
○ every caller
○ Emergency

... do the following:

● connect
○ deny
○ ◆divert to:
○ require surety of $10 and connect
○ require subject and connect
○ let caller decide
○ require caller ID

Text to send: -

Multilateral Security considers conflicts

Respecting Interests

- Parties can define their own **interests.**
- Conflicts can be **recognized** and **negotiated.**
- Negotiated **results** can be reliably **enforced.**

Supporting Sovereignty

- Requiring each party to **only minimally trust** in the honesty of **others**
- Requiring **only minimal or no trust in technology** of others

Protection of **different parties** and their **interests**

Reachability Management and Multilateral Security

- Protection of callers and callees
- Balance of security requirements
- Processing and storage of sensitive data in a personal environment

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

Outline of this course

Lectures and Exercises

12-Apr-16	L01	Introduction	Lecture
13-Apr-16	L02	Authentication	Lecture
19-Apr-16	E01	Authentication	Exercise
26-Apr-16	L03	Access Control	Lecture
27-Apr-16	G01	Guest Lecture by Jürgen Kühn (PWC)	Guest Lecture
03-May-16	L04	Cryptography I	Lecture
10-May-16	L05	Cryptography II	Lecture
11-May-16	E02	Access Control	Exercise
17-May-16	L06	Electronic Signatures	Lecture
24-May-16	L07	Identity Management	Lecture
25-May-16	L08	Privacy protection	Lecture
31-May-16	G02	Information security management	Guest Lecture
07-Jun-16	L09	Computer System Security	Lecture
08-Jun-16	L10	Network Security I	Lecture
14-Jun-16	E03	Cryptography	Exercise
21-Jun-16	G03	Guest lecture by Daniel Hamburg	Guest Lecture
22-Jun-16	UE04	Guest lecture by Jens Eichler	Guest Lecture
28-Jun-16	L11	Network Security II	Lecture
05-Jul-16	L12	Security Engineering	Lecture
06-Jul-16	L13	Social Engineering exercises	Exercise
12-Jul-16	UE08	Exam prep and wrap up	Lecture and Q&A

MSc Thesis

- **Title**
  - **Detection, Quantification and Prevention of Privacy Risks: A Literature Review**
- **Introduction**
  - Recent scandals and increased privacy concerns
  - Efforts to tackle privacy revelations
    - frameworks for quantifying privacy damages,
    - machine-learning techniques for predicting privacy risks
    - utilizing anonymization technologies for privacy prevention.
- **Approach**
  - Systematic review of literature relevant to the topic by using academic search engines and publication portals such as IEEE Xplore, Elsevier, ACM, Springer, Google Scholar, etc.
- **Expected Results**
  - Thorough review of literature relevant to the theme of the topic.
  - Classification of literatures into subfields within the problem domain.
  - Identifying open research areas, preparing recommendations on methodologies

Biometrics in Online Banking - Questionnaire

http://biometrics-user.limequery.com/index.php/566836/lang-en