Information & Communication Security (SS 15)

Introduction

Dr. Jetzabel Serna-Olvera
@sernaolverajm
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching and Research Agenda
- Introduction into information and communication security
- Outline of this Course

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 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

Markus Tschersich

Stephan Heim

Shuzhe Yang

Lars Wolos

Team

Marvin Hegen

Ahmad Sabouri

Fatbardh Veseli

Gökhan Bal

Christopher Schmitz

Welderufael Tesfay

Ahmed Yesuf

Research Fellows & External PhD Students

Mike Radmacher

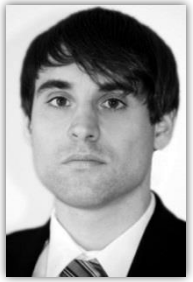
Andreas Albers

Stefan Weiss

Christian Kahl

André Deuker

Sascha Koschinat



Andreas Leicher

Tim Schiller

Niels Johannsen

Thomas Leiber

Christian Weber

Team

Office:

Elvira Koch

Email: elvira.koch@m-chair.de

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

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

Dr. Jetzabel Serna-Olvera

Projects

Security

Smart Cybercrime Data Collection and Exchange
+
Mobile Banking Security

Coordination improvement by best practices

Research in Migration Management Technologies

Identity Management

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

Identity Management in Digital Territories

Federated Identity Management based on Liberty

Social Networks

Methods and Technologies for Social Media

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

Teaching in Frankfurt

Teaching Topics

- Identity Management
- Privacy
- ICT Security
- Mobile Business
- Business Informatics

Master Courses

Lectures

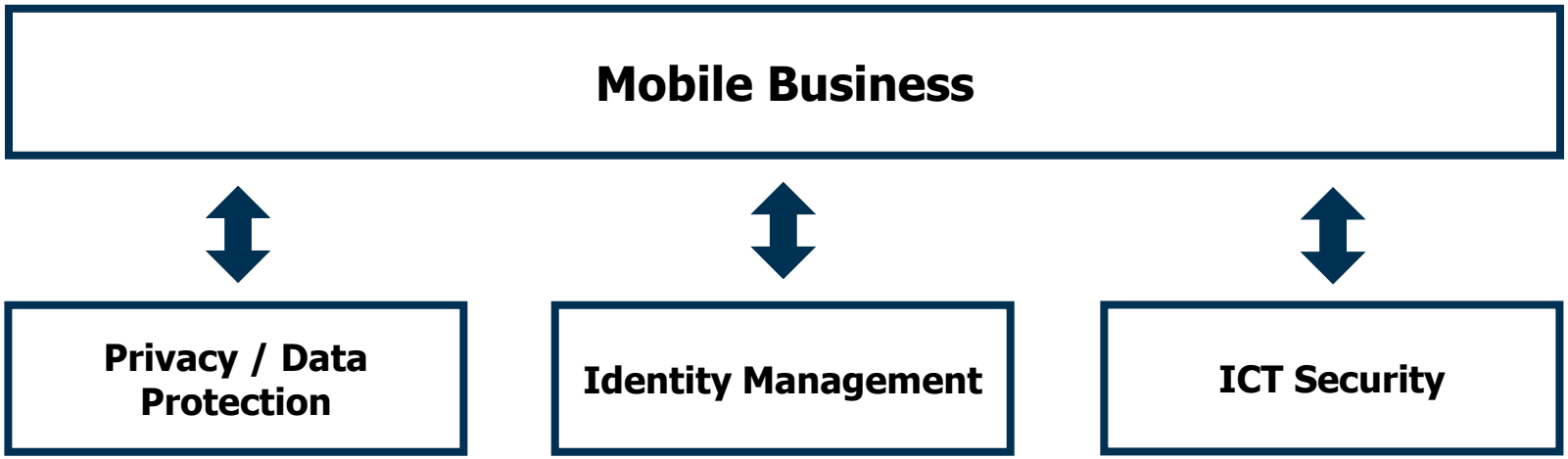
- Mobile Business 1
- Mobile Business 2
- I & C Security
- Privacy vs. Data
- Seminars
- Master Thesis

Bachelor Courses

Lectures

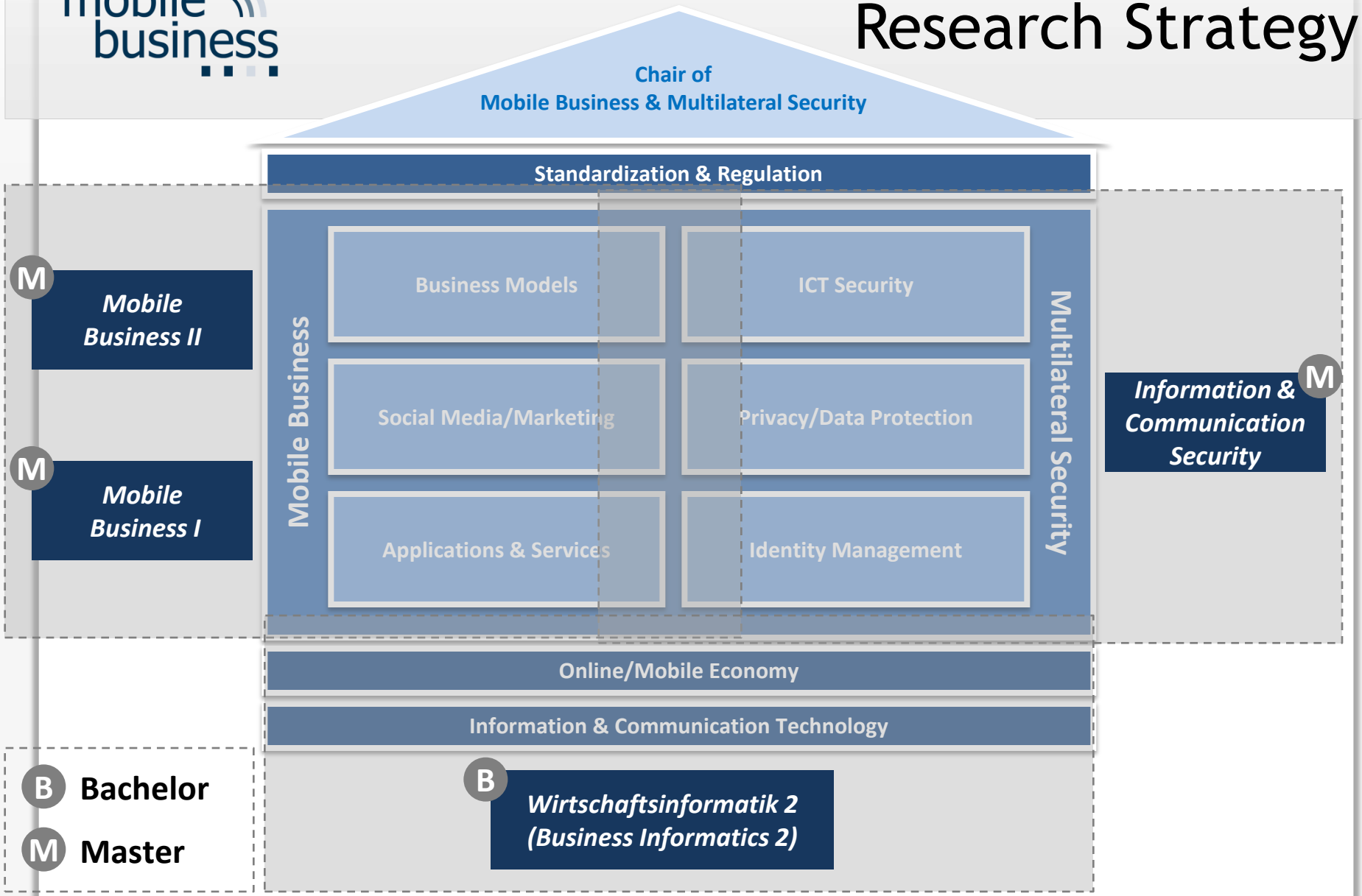
- Business Informatics 2
- Seminars
- Bachelor Thesis

M-Chair Research Statement



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



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. Fatbardh Veseli

RuW Building, Office 2.232

Phone: 069 / 798 - 34704

Email: fatbardh.veseli@m-chair.de

M.Sc. Welderufael B. Tesfay

RuW Building, Office 2.232

Phone: 069 / 798 - 34706

Email: welderufael.tesfay@m-chair.de

twitter.com/mchair

sec@m-chair.de

Fatbardh Veseli

Research Assistant

General Research Interests:

- Privacy enhancing technologies – challenges and opportunities
- User-centric identity management
- Security and privacy evaluation frameworks
- Technologies for Privacy-respecting eID schemes

Projects:

- Attribute-Based Credentials for Trust (ABC4Trust)

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:

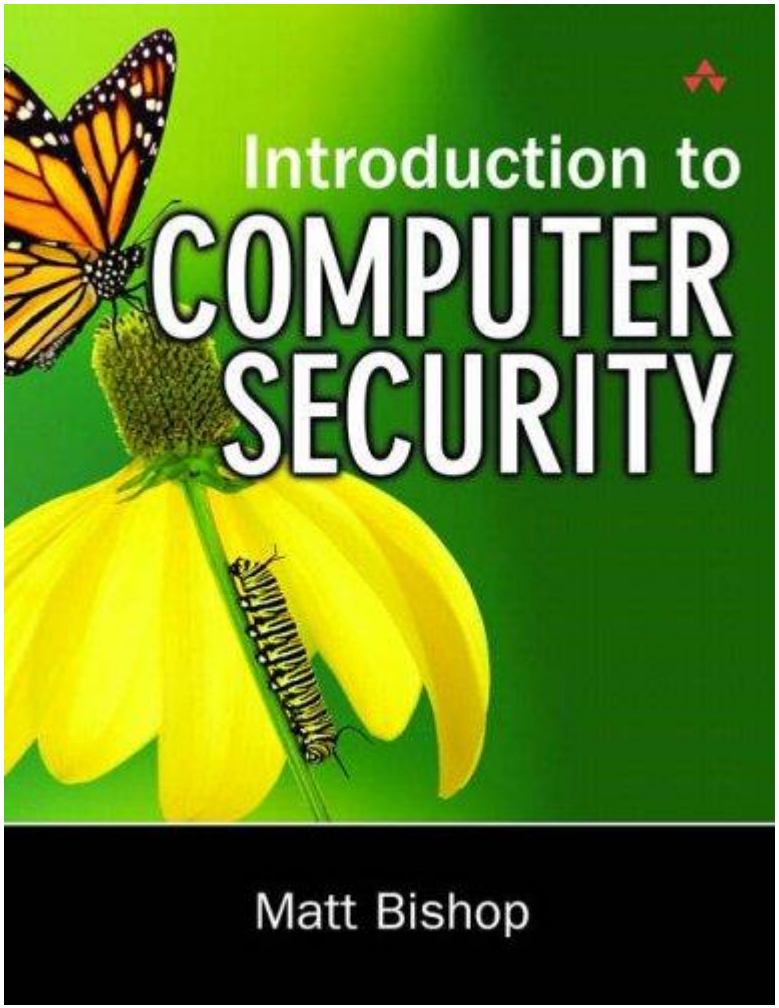
- Usable Privacy Enhancing Technologies with Focus on Privacy-ABCs
- Learning from User Data to Enhance User Privacy

Projects:

- Attribute-based Credentials for Trust (ABC4Trust)

mobile business

Literature



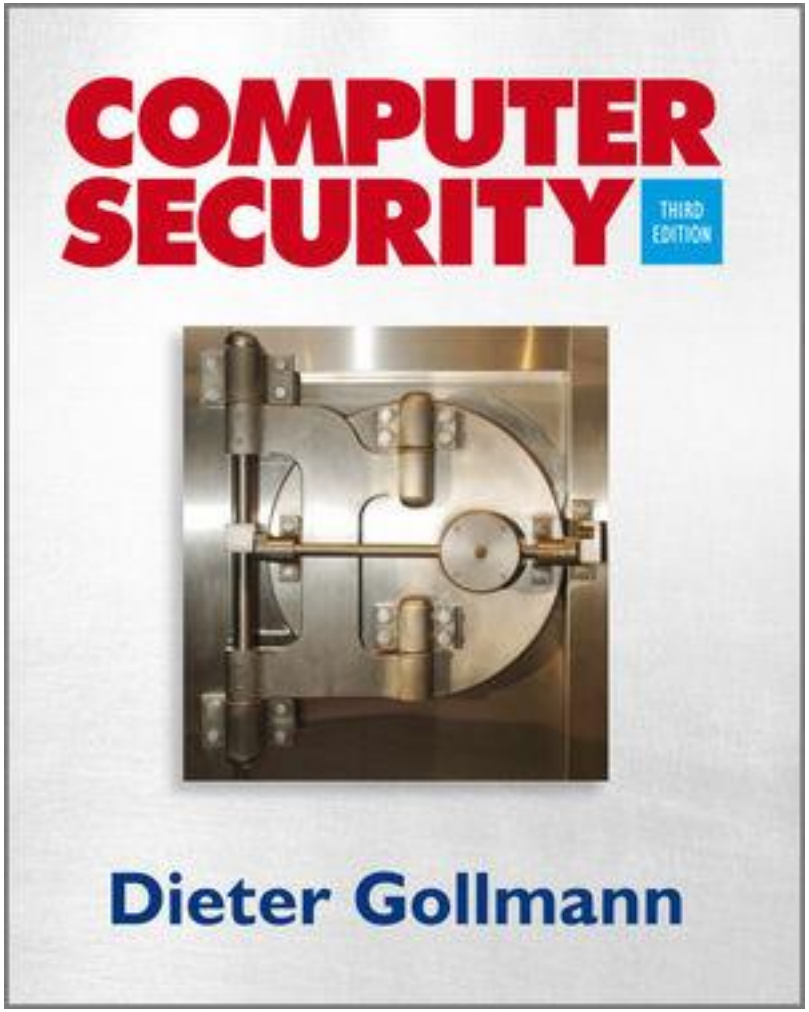
Matt Bishop:

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

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

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

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: http://www.m-chair.de/index.php?option=com_teaching&view=lecture&id=10

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

March 5, 2012, 3:40PM

Hacker Group Breaches Library of Congress Site, Publishes Passwords

Risks of Unprotected Market Activities

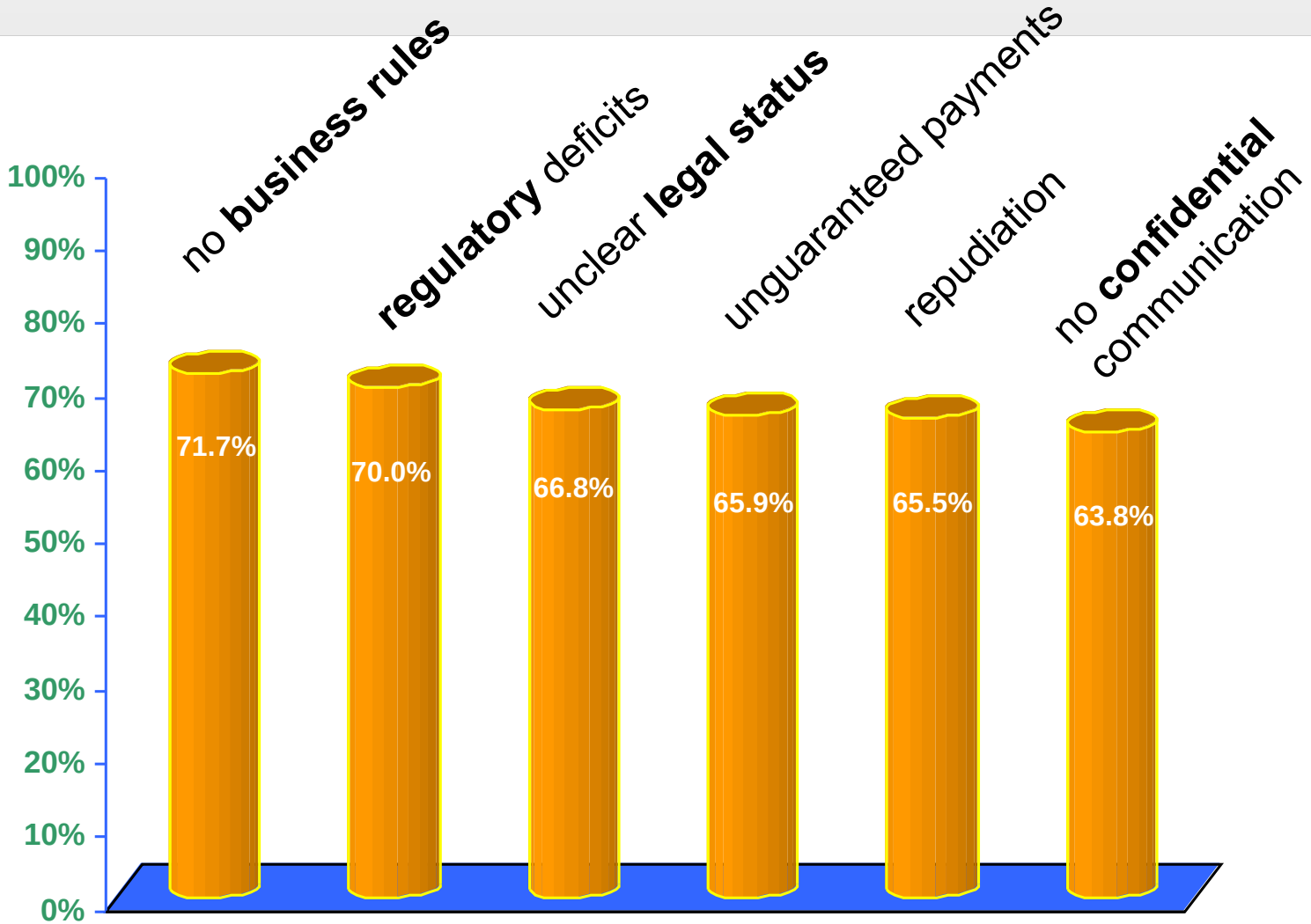
Provider

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

Consumer

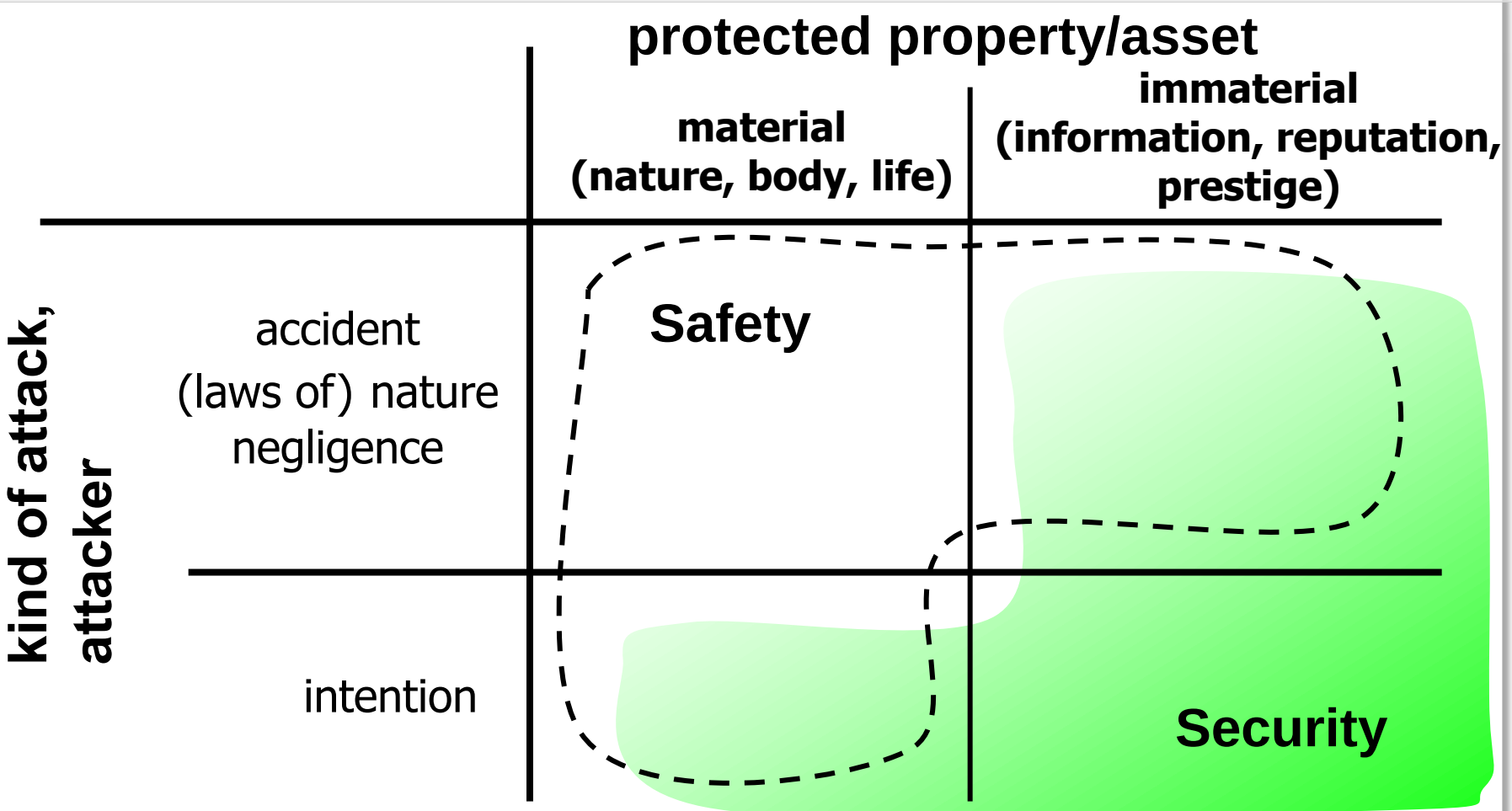
- unwanted deliveries (false, not ordered, …)
- unauthorized / unexpected direct debt of money, e.g. from a credit card account
- unwanted advertising mail (“spamming”)
- transparent consumers
- …

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



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)

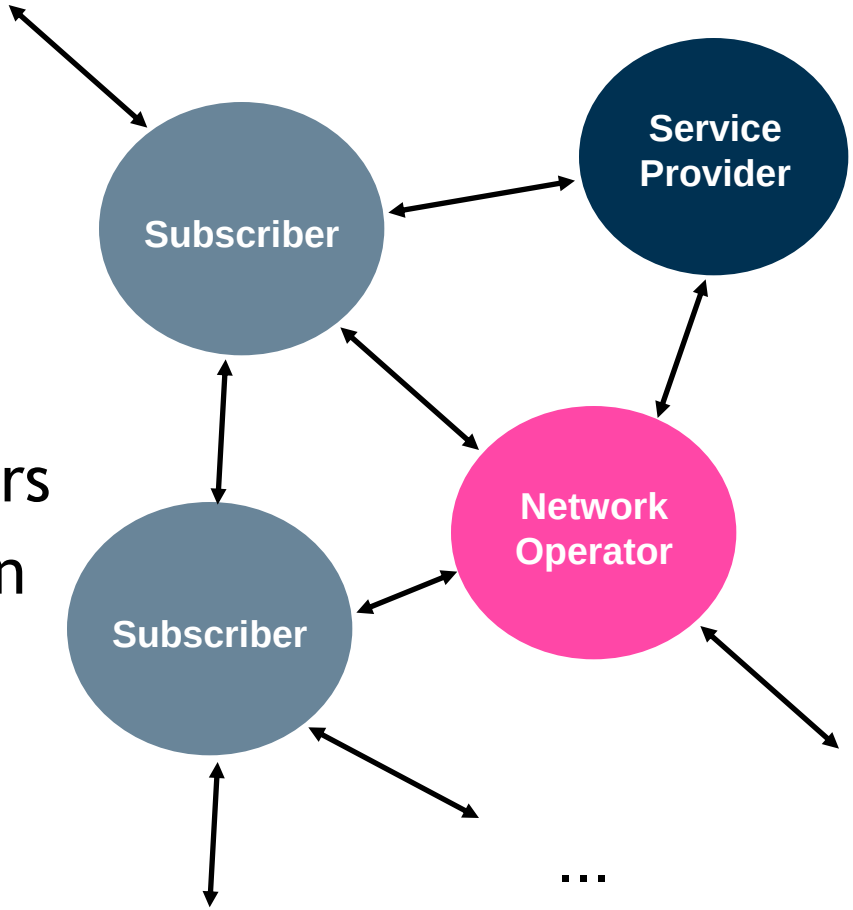
- ***Unauthorized impair of functionality***, that means loss of **availability**: If the medical history is accessible solely via one network and this network has a breakdown when patient data has to be queried it may be life-threatening for the patient.

- ***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

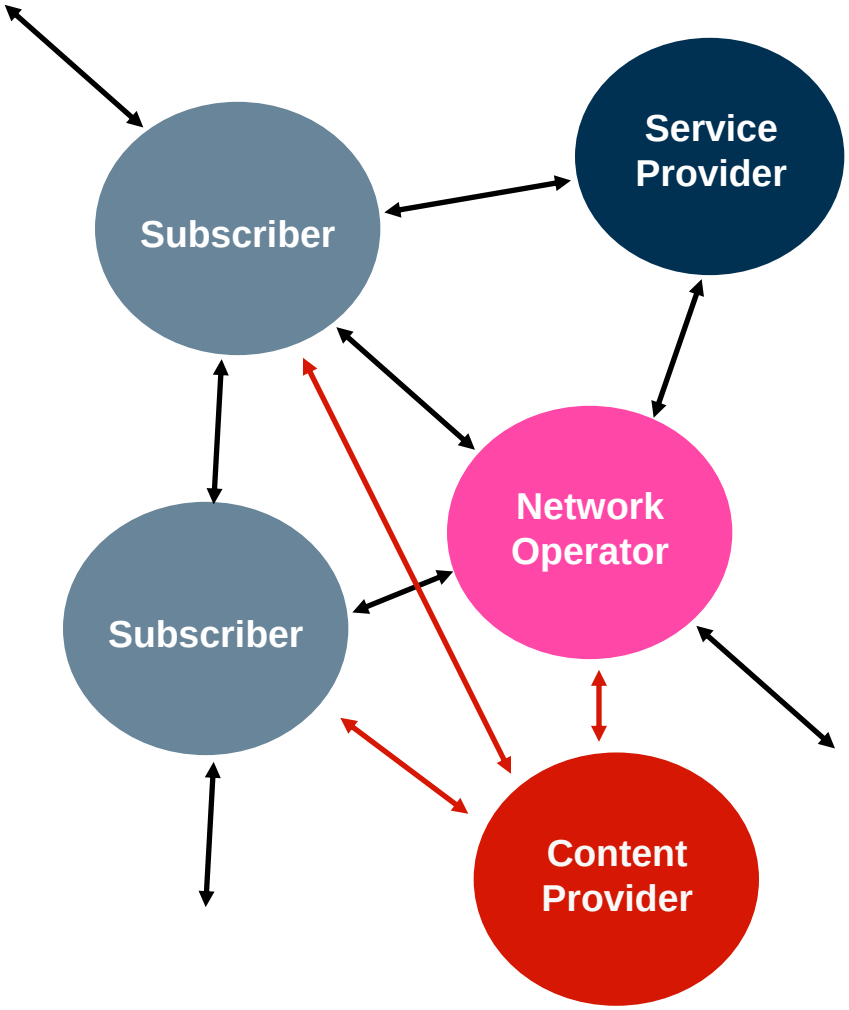
- Customers/Merchants
- Communication partners
- Citizens/Administration



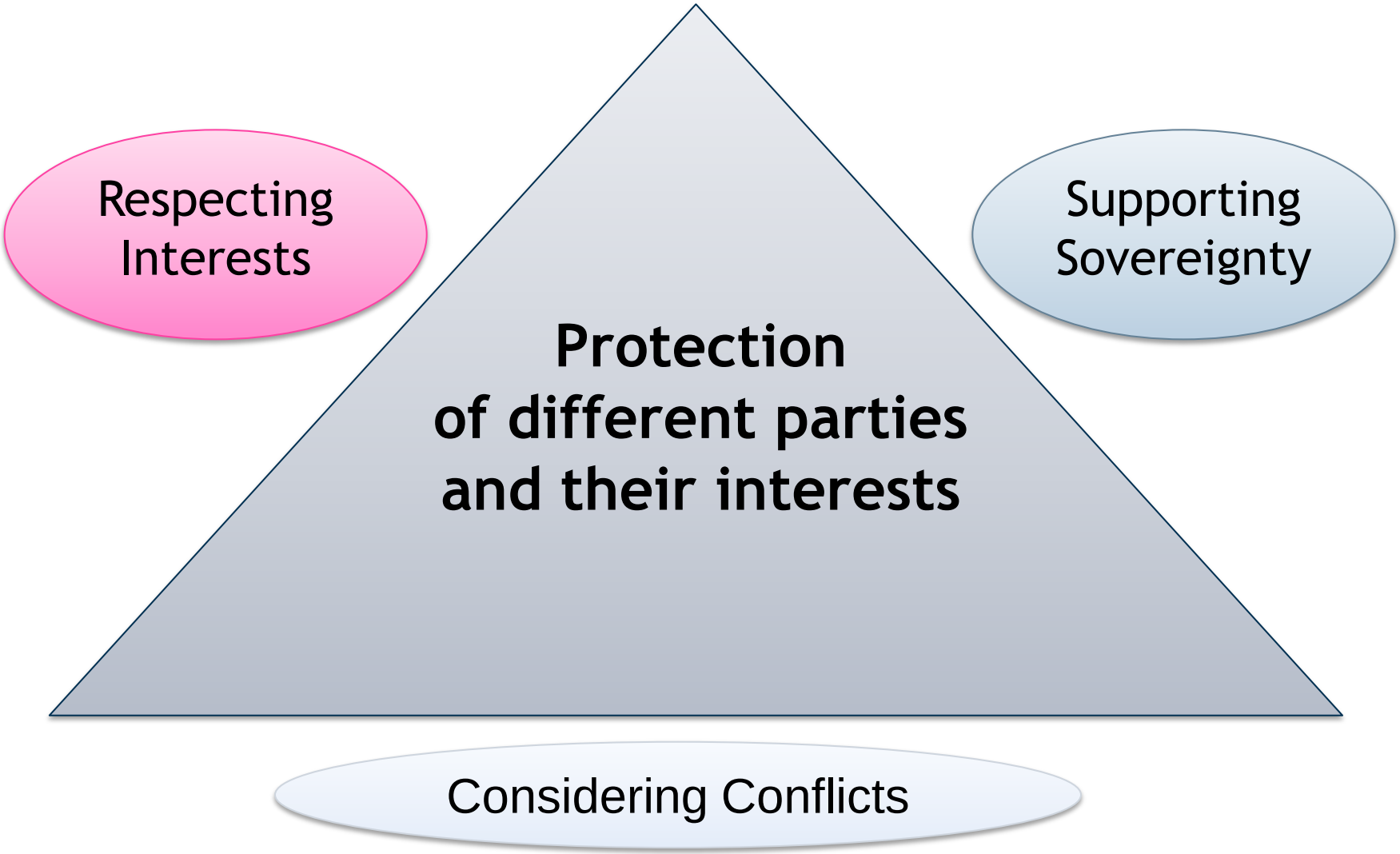
Multilateral Security

… in a world of consortia

- more partners
- more complex relations



Multilateral Security



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

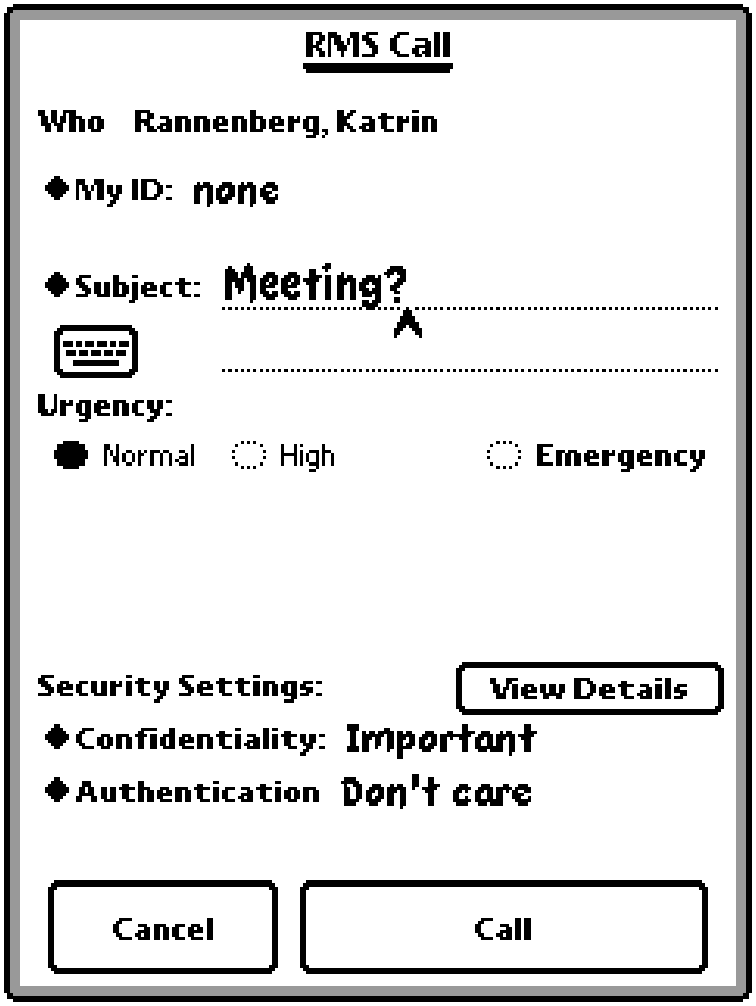
Call

Call

Negotiation

Topics of Negotiation

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



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

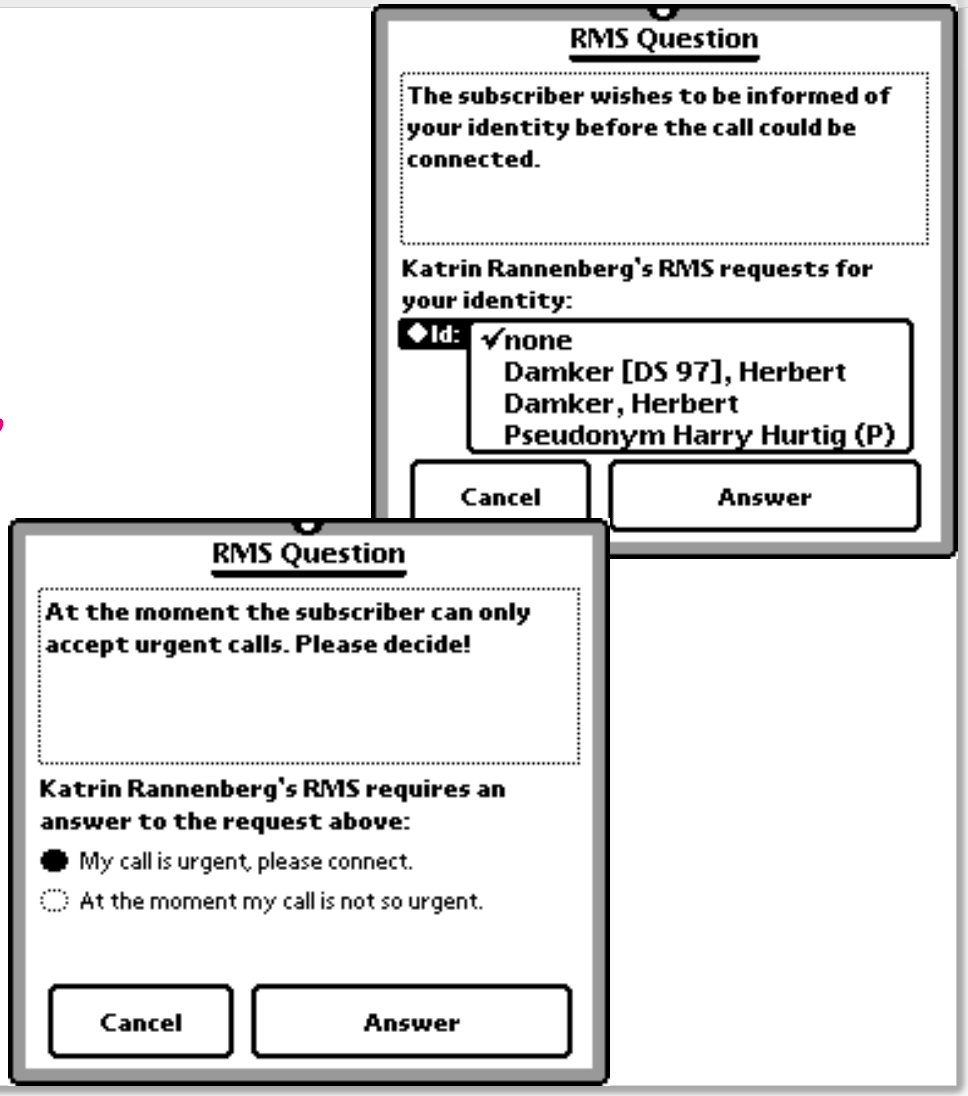
"I welcome you calling back.

Provision of a reference

"My friends are your friends!

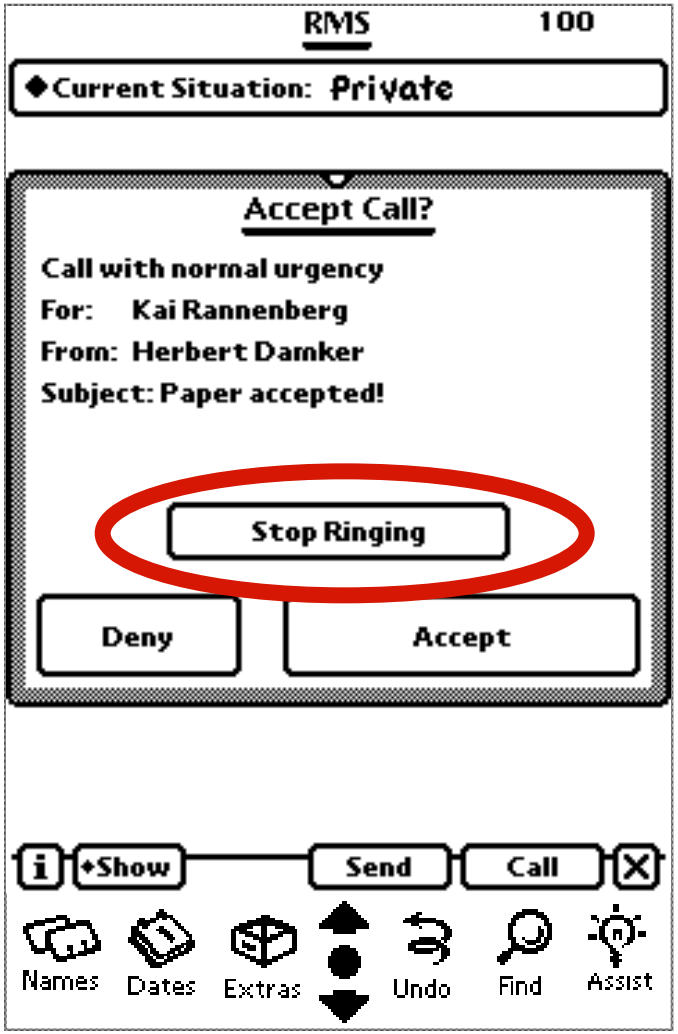
Offering a surety

"Satisfaction guaranteed
or this money is yours!"



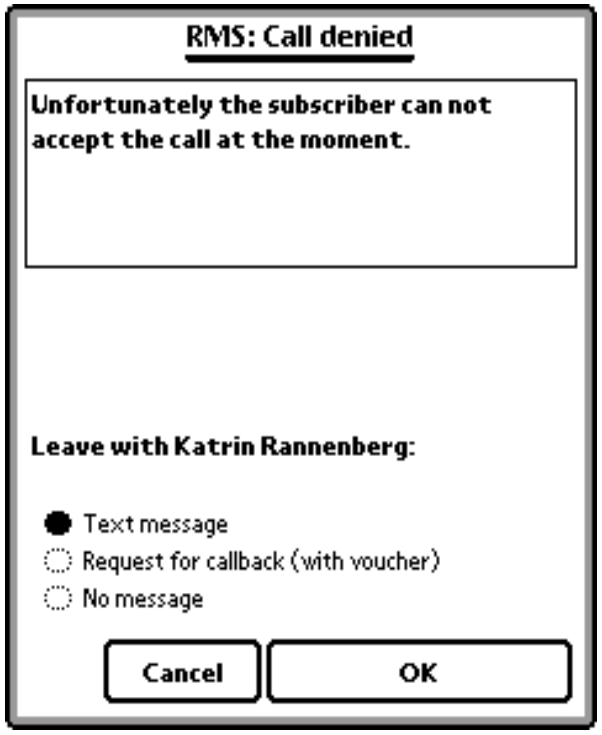
RMS accepted call (Callee display)

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



RMS denied call (Caller display)

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



Configuring your RMS

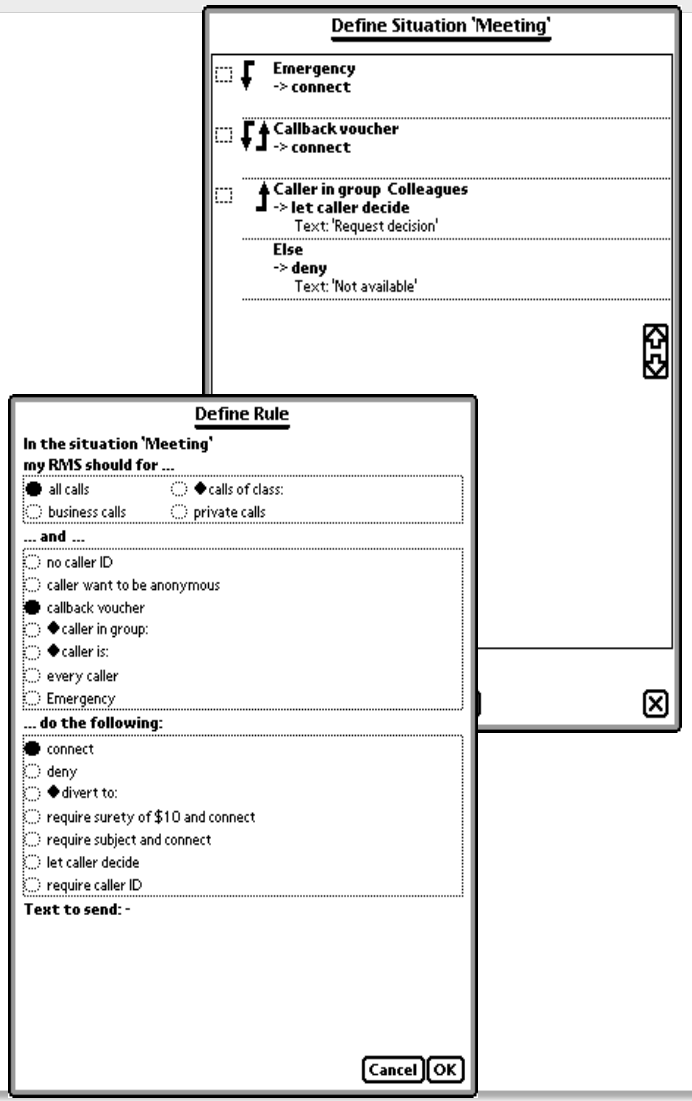
Situations

Set of rules how to deal with an incoming call

Rules

Combination of features

Users can reconfigure initial rules and situations as they like.



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 (1)

Tuesday	14-Apr-15	14:00-16:00	HZ 7	Introduction
Tuesday	21-Apr-15	14:00-16:00	HZ 7	Authentication
Wednesday	22-Apr-15	10:00-12:00	HZ 7	Access Control
Tuesday	28-Apr-15	14:00-16:00	HZ 7	Authentication
Tuesday	05-May-15	14:00-16:00	HZ 7	Cryptography I
Wednesday	06-May-15	10:00-12:00	HZ 7	Cryptography II
Tuesday	12-May-15	14:00-16:00	HZ 7	Guest Lecture 1 - Juergen Kuehn - Biometrics
Tuesday	19-May-15	14:00-16:00	HZ 7	Access Control
Wednesday	20-May-15	10:00-12:00	HZ 7	Electronic Signatures
Tuesday	26-May-15	14:00-16:00	HZ 7	Cryptography
Tuesday	02-Jun-15	14:00-16:00	HZ 7	Identity Management

mobile business

Lectures and Exercises

Outline of this course (2)

Wednesday	03-Jun-15	10:00-12:00	HZ 7	Privacy protection
Tuesday	09-Jun-15	14:00-16:00	HZ 7	Computer System Security
Tuesday	16-Jun-15	14:00-16:00	HZ 7	Network Security I
Wednesday	17-Jun-15	10:00-12:00	HZ 7	Network Security II
Tuesday	23-Jun-15	14:00-16:00	HZ 7	Guest lecture 2 - Ronny John - Payment Security
Tuesday	30-Jun-15	14:00-16:00	HZ 7	Guest lecture 3 - Dr.Daniel Hamburg - Pentesting
Wednesday	01-Jul-15	10:00-12:00	HZ 7	Guest Lecture 4 - Jens Eichler - Social engineering
Tuesday	07-Jul-15	14:00-16:00	HZ 7	Security Engineering
Tuesday	14-Jul-15	14:00-16:00	HZ 7	Evaluation Criteria
Wednesday	15-Jul-15	10:00-12:00	HZ 7	Exam prep and wrap up

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Jetzabel M. Serna-Olvera
Goethe University Frankfurt
E-Mail: Jetzabel.Serna-Olvera@m-chair.de
WWW: www.m-chair.de