

Information & Communication Security (WS 2016/17)

Introduction

Prof. Dr. Kai Rannenberg

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

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

Business Informatics @ Goethe University Frankfurt

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

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





Kai Rannenberg



Jetzabel
Serna-Olvera



Sebastian
Pape



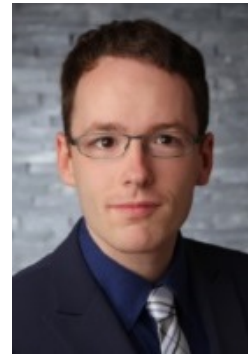
Fatbardh
Veseli



Welderufael
Tesfay



Ahmed S. Yesuf



Christopher
Schmitz



David Harborth

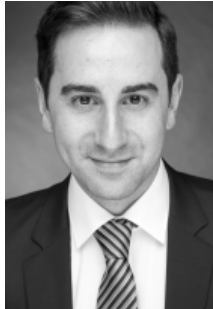


Majid
Hatamian

Research Fellows & External PhD Students



Shuzhe Yang



Gökhan Bal



Mike
Radmacher



Andreas
Albers



Stefan
Weiss



André
Deuker



Markus
Tschersich



Sascha
Koschinat



Stephan Heim



Lars Wolos



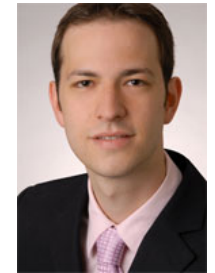
Tim
Schiller



Niels
Johannsen



Ahmad Sabouri



Marvin Hegen

Office:

Elvira Koch

Email: elvira.koch@m-chair.de

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



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

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

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

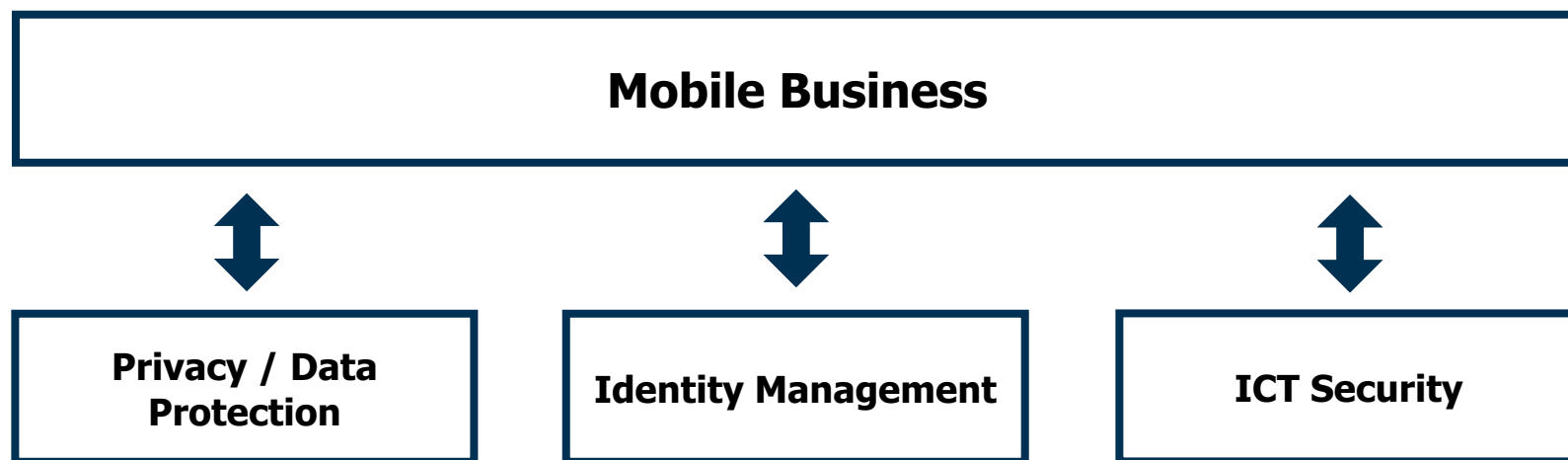
Bachelor Courses

Lectures

Business Informatics 2

Seminars

Bachelor Thesis



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

Chair of
Mobile Business & Multilateral Security

Standardization & Regulation

M Mobile Business II

Business Models

ICT Security

Social Media/Marketing

Privacy/Data Protection

M Mobile Business I

Applications & Services

Identity Management

M Information & Communication Security

Mobile Business

Multilateral Security

Online/Mobile Economy

Information & Communication Technology

B Bachelor

M Master

B Wirtschaftsinformatik 2
(Business Informatics 2)

- **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

- 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



twitter.com/mchair



sec@m-chair.de

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



Research Interests:

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

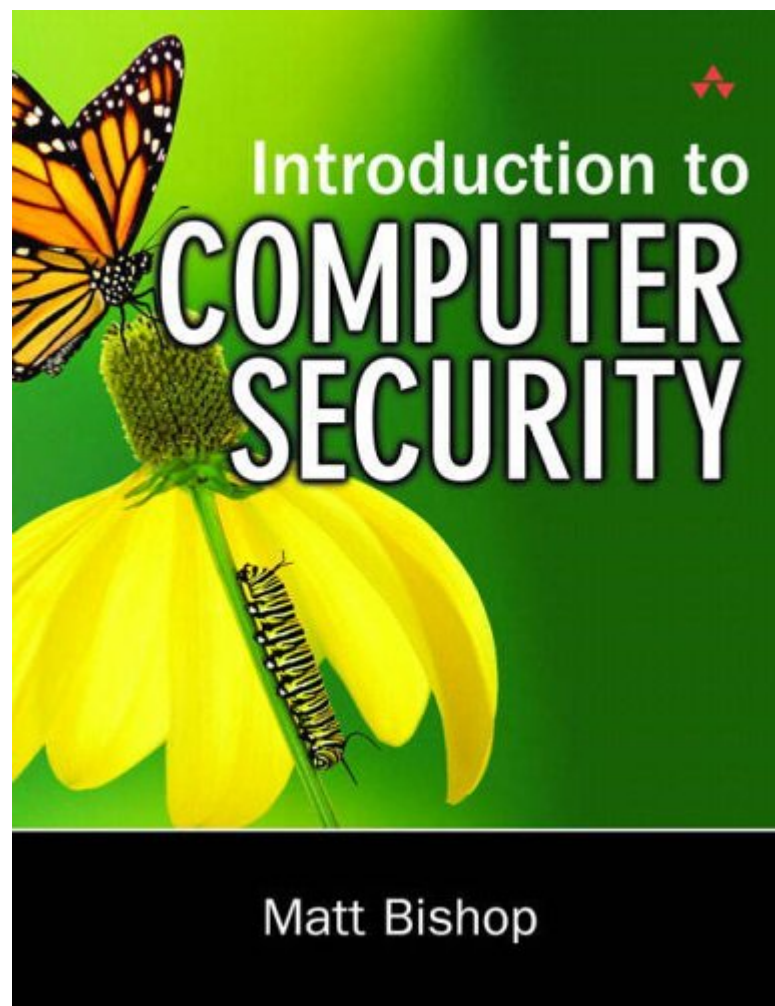
PhD Focus:

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

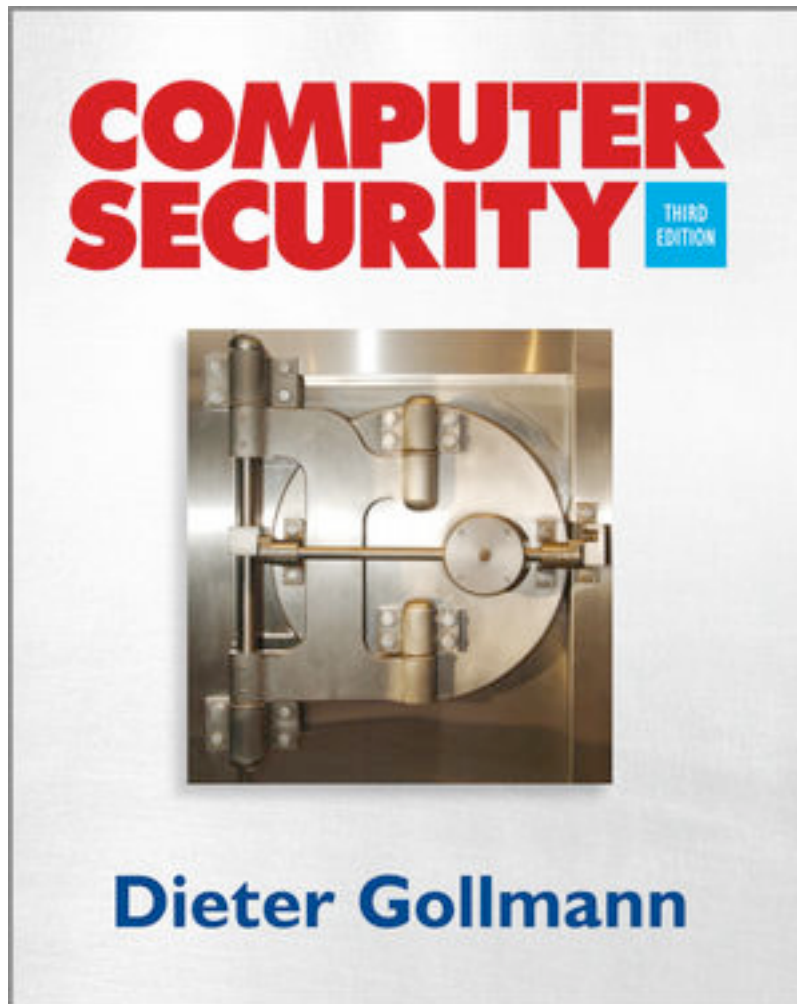
Projects:

- CREDENTIAL





Matt Bishop:
Introduction to
Computer Security
Addison Wesley
ISBN: 0-321-24744-2



Dieter Gollmann:
Computer Security
John Wiley & Sons
ISBN: 0-470-74115-5

Oldenbourg Verlag

Claudia Eckert

IT-Sicherheit

Konzepte – Verfahren – Protokolle

7. Auflage



In German:

Claudia Eckert:

IT-Sicherheit

Oldenbourg

ISBN: 978-3-486-70687-1

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



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=26

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

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 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

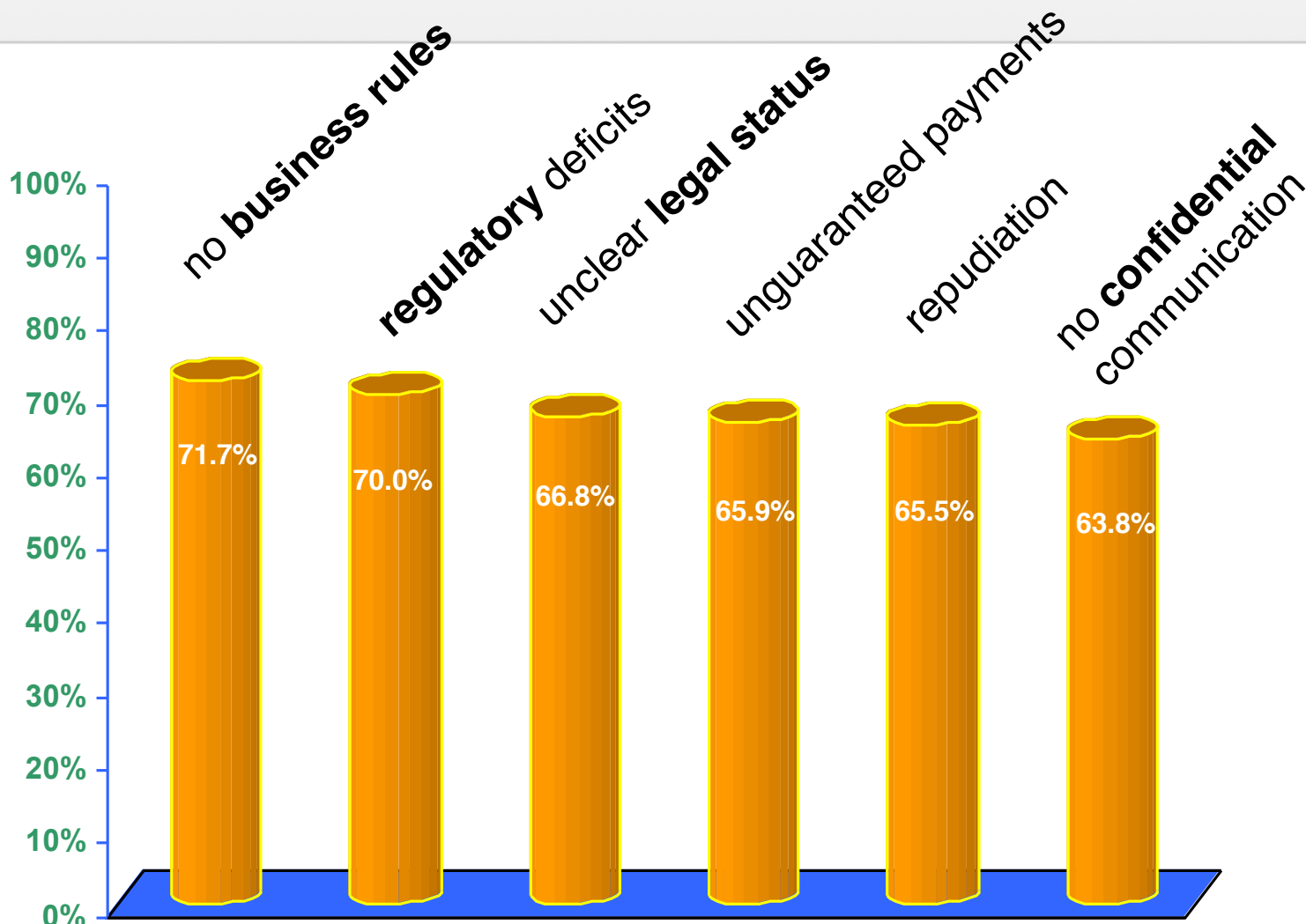
Provider

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

Consumer

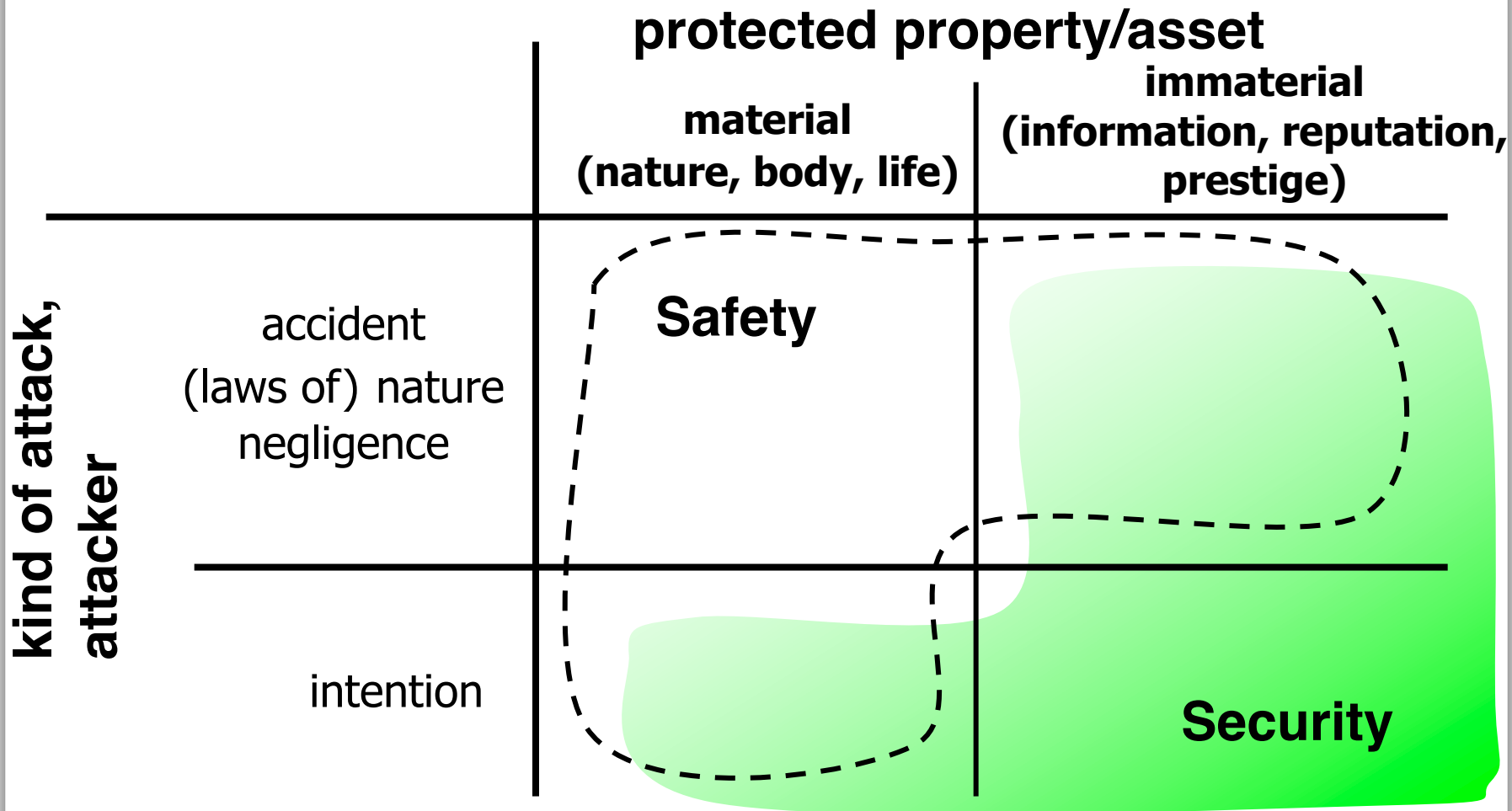
- unwanted deliveries (false, not ordered, ...)
- unauthorized / unexpected direct debt of money, e.g. from a credit card account
- unwanted advertising mail (“spamming”)
- transparent consumers
- ...

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



A very human discrepancy

- **Privacy**
Protect the own sphere and the own values/assets
- **Binding**
Gain trust (of partners), transfer values

A 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 always accountable to responsible parties

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

- ***Unauthorized acquisition of information*** = 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).
- Citizens (in smart cities) should not be monitored or tracked by default.

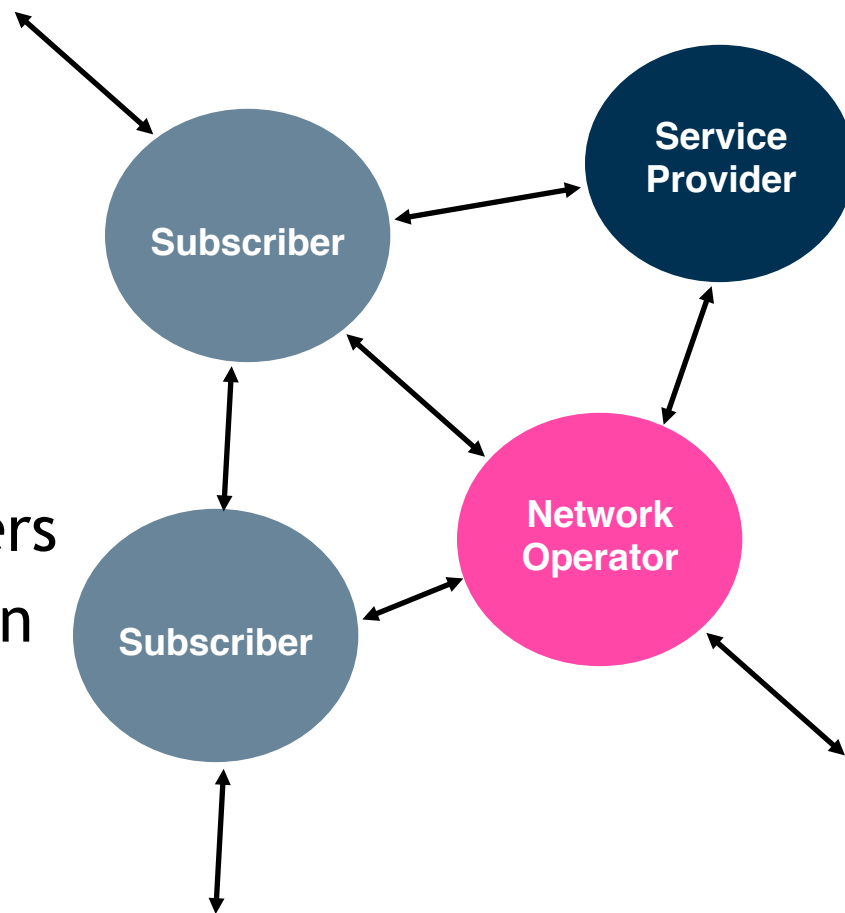
- ***Unauthorized modification*** of information = loss of **integrity**:
- Unauthorized and unobserved data modifications (e.g. a prescription, a medicament ordering or a dosage instruction) may lead to life-threatening consequences.
- Forging of electronic records can create chaos in society - often discussed as informational warfare.
- Manipulation of traffic regulation and control in (smart) cities is a nuisance and can even be life-threatening.

- ***Unauthorized impair of functionality*** = loss of **availability**:
- If a patient's medical record is accessible solely via one network and this network fails, when patient data is needed, this may be life-threatening for the patient.
- (Smart) cities have a major problem, if critical infrastructures for e.g. electricity distribution are not available anymore.

- ***No responsible parties for actions*** = loss of **accountability**:
- If the persons liable for procedures in medical ICT systems (e.g. for the delivery of diagnoses, therapy instructions or billings) cannot be identified, irresponsible actions may occur.
- The consequences of a mistake may be worse for the injured party since it is unclear whom to ask for compensation.
- If (restrictive) measures (e.g. traffic suspension) taken in smart cities cannot be attributed to responsible parties (“the computer has decided”) citizens lose trust.

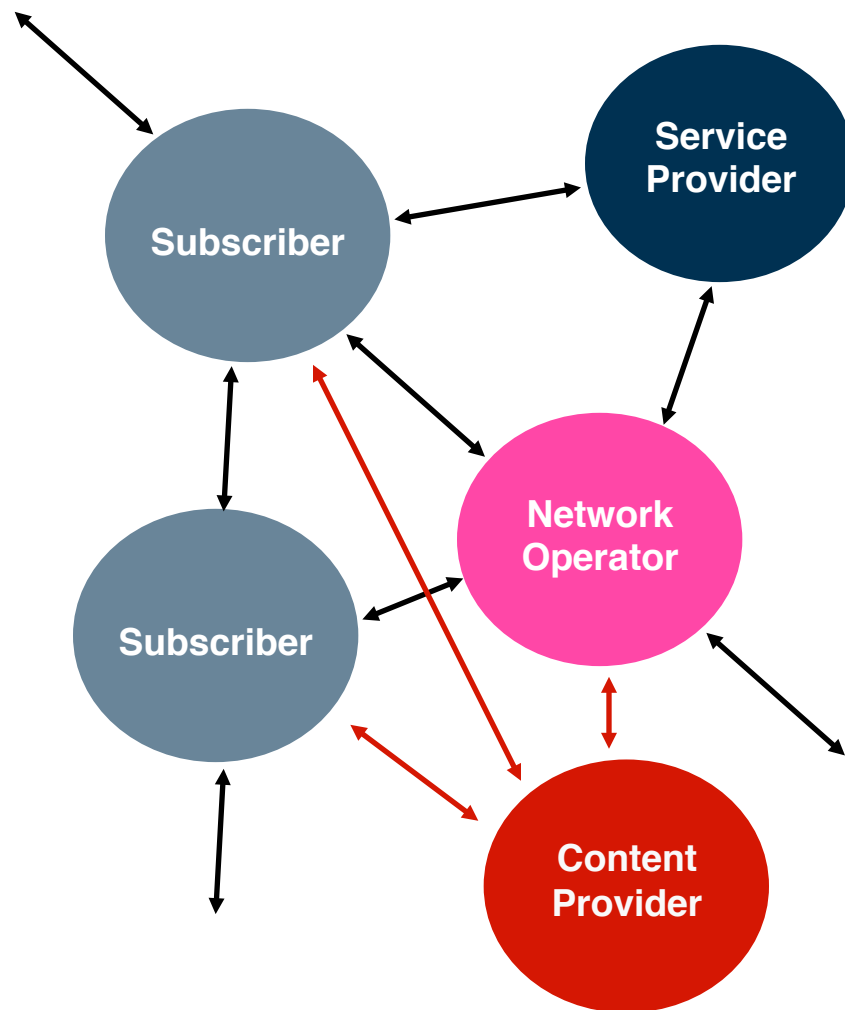
Different Parties with different Interests

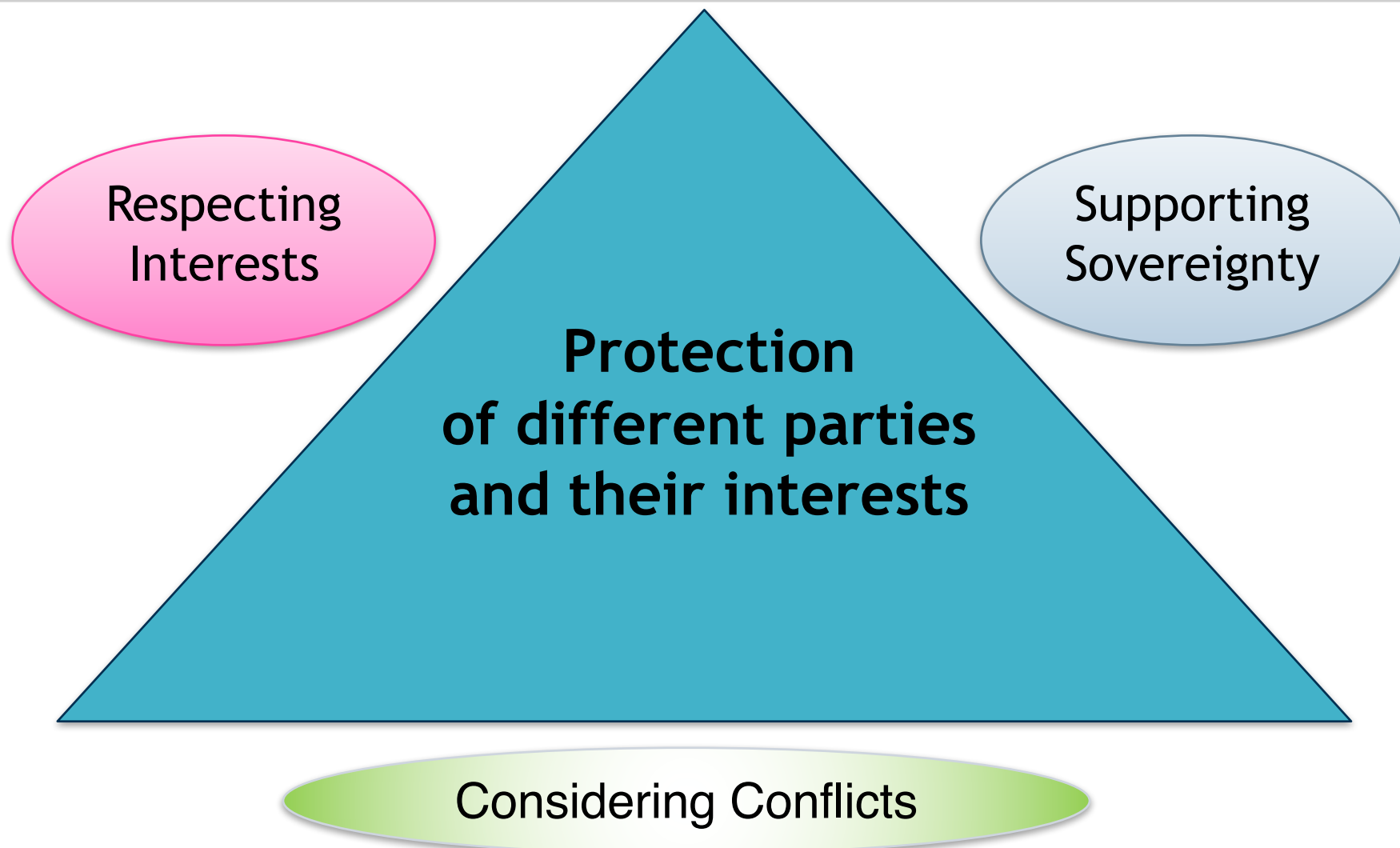
- Customers/Merchants
- Communication partners
- Citizens/Administration



... in a world of
consortia

- more partners
- more complex relations





Respecting Interests

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

Supporting Sovereignty

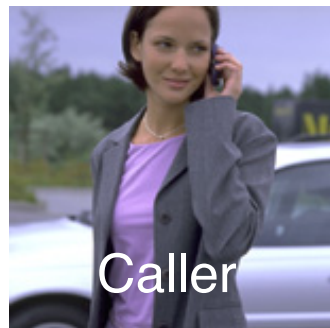
- Requiring each party to **only minimally trust** in the honesty of **others**
- Requiring **only minimal or no trust** in **technology** of others

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

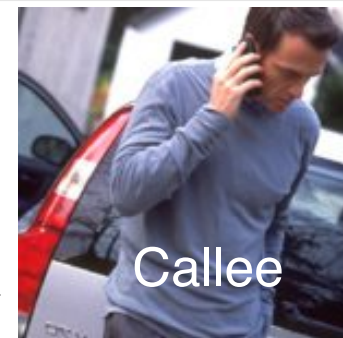
Multilateral Security in daily communication

The Challenge

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



accept



or

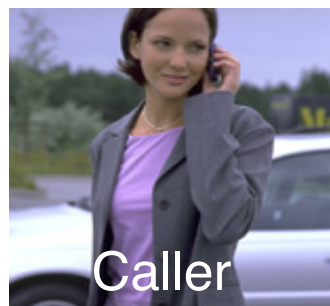
deny



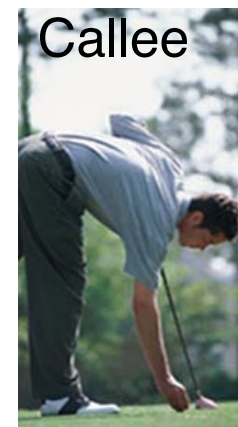
→ Reachability Management (RM)

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



Negotiation



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: [View Details](#)

◆ **Confidentiality:** Important

◆ **Authentication:** Don't care

[Cancel](#) [Call](#)

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)

Cancel Answer

RMS Question

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

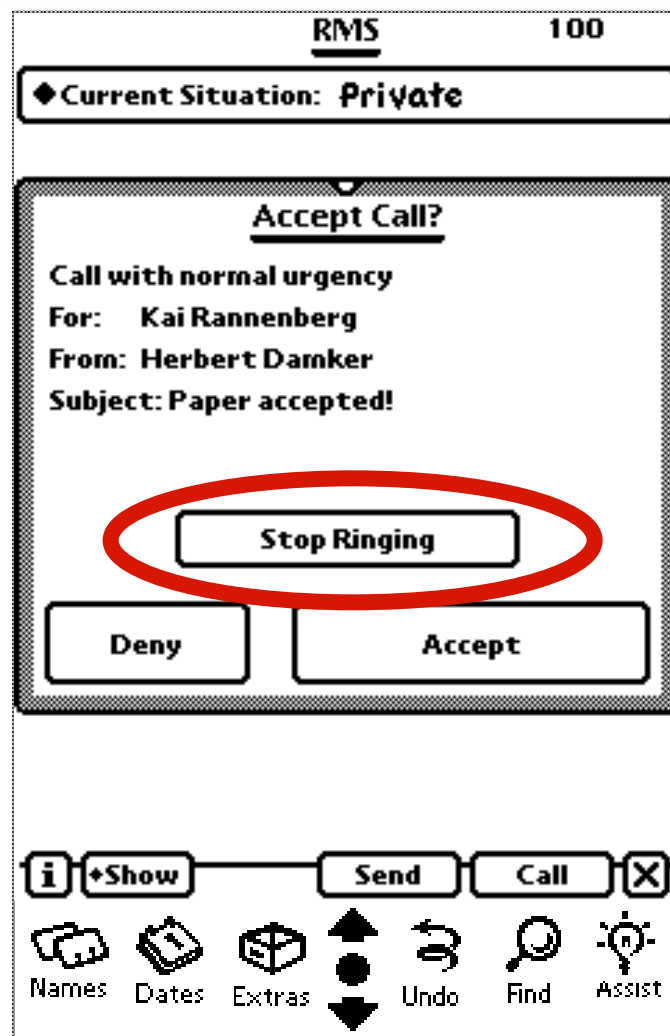
Katrin Rannenberg's RMS requires an answer to the request above:

My call is urgent, please connect.
 At the moment my call is not so urgent.

Cancel Answer

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

RMS: Call denied

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

Leave with Katrin Rannenber:

Text message
 Request for callback (with voucher)
 No message

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: -

Cancel OK

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**

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

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

Lectures and Exercises

Outline of this course

| | | |
|----------------|--|---------------|
| 18-Oct-16 VL1 | Introduction | Lecture |
| 19-Oct-16 VL2 | Authentication | Lecture |
| 26-Oct-16 Ü1 | Authentication | Exercise |
| 01-Nov-16 VL3 | Access Control | Lecture |
| 02-Nov-16 VL4 | Cryptography I | Lecture |
| 09-Nov-16 VL5 | Cryptography II | Lecture |
| 15-Nov-16 Ü2 | Access Control | Exercise |
| 16-Nov-16 G1 | Guest Lecture by Jürgen Kühn (SVA System Vertrieb Alexander) | Guest Lecture |
| 23-Nov-16 VL6 | Electronic Signatures | Lecture |
| 29-Nov-16 VL7 | Identity Management | Lecture |
| 30-Nov-16 Ü3 | Cryptography I | Exercise |
| 07-Dec-16 VL8 | Privacy Protection I | Lecture |
| 13-Dec-16 Ü4 | Cryptography II | Exercise |
| 14-Dec-16 VL9 | Privacy Protection II | Lecture |
| 21-Dec-16 VL10 | Computer System Security | Lecture |
| 10-Jan-17 G2 | Guest Lecture by Jens Eichler (RühlConsulting) | Guest Lecture |
| 11-Jan-17 G3 | Guest Lecture by Amir Neziri (Lufthansa) | Guest Lecture |
| 18-Jan-17 VL11 | Network Security I | Lecture |
| 24-Jan-17 VL12 | Network Security II | Lecture |
| 25-Jan-17 G4 | Guest Lecture by Dr. Daniel Hamburg (TÜVRheinland) | Guest Lecture |
| 01-Feb-17 VL13 | Security Engineering | Lecture |
| 07-Feb-17 VL14 | Evaluation Criteria | Lecture |
| 08-Feb-17 Ü5 | Exam prep and wrap up | Exercise |