mobile business

Lecture 01

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (SS 2024)

Introduction

Prof. Dr. Kai Rannenberg,

Sascha Löbner

Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- 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	**Mobile Business & Multilateral Security** Prof. Dr. Kai Rannenberg	**Business Education** (associated) Prof. Dr. Eveline Wuttke
Information Systems & Information Management Prof. Dr. Wolfgang König	**Business Informatics & Microeconomics** Prof. Dr. Lukas Wiewiorra	**Business Informatics & Information Management** Prof. Dr. Oliver Hinz

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

Chair of Mobile Business & Multilateral Security

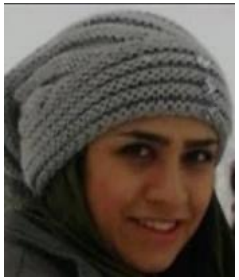
Theodor-W.-Adorno-Platz 4
Campus Westend
RuW, 2nd Floor

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

www.m-chair.de

Team & PhD Students

Kai Rannenberg



Narges Arastouei

Diana Weiss

Sascha Löbner

Atiyeh Sadeghi

Ann-Kristin Lieberknecht

Frédéric Tronnier

Ahad Niknia

Peter Hamm

Tim Schiller

Michael Schmid

Christopher Schmitz

Selected Alumni

Prof. Dr. Jan Muntermann
Göttingen University

Dr. Stefan Figge
Buyln (Deutsche Telekom / Orange)

Dr. Mike Radmacher
Deutsche Telekom

Dr. Andreas Albers
Deutsche Telekom

Dr. Stefan Weiss
Swiss Re

Prof. Dr. Denis Royer
Ostfalia - Hochschule für angewandte Wissenschaften

Dr. Markus Tschersich
Continental

Dr. Ahmad Sabouri
Continental

Dr. Falk Wagner
EE

Dr. Christian Kahl
CyberSolutions GmbH

Dr. Gökhan Bal
Deutsche Bahn

Dr. André Deuker
KfW

Dr. Shuzhe Yang
GLS

Dr. Ahmed Yesuf
FARO

Dr. Welderufael Tesfay
Deutsche Telekom

Dr. Fatbardh Veseli
Capgemini Germany

Dr. Majid Hatamian
Google

Dr. habil. Sebastian Pape
Continental

Dr. *David Harborth*
Capgemini Invent

Team

Office:

Diana Weiß
Office Hours: On appointment
RuW Building, Office 2.257
Email: diana.weiss@m-chair.de

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

Kai Rannenberg

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 at Goethe University Frankfurt at the Faculty of Business and Economics (FB02)
- Since 2012-04 Visiting Professor at the National Institute for Informatics (Tokyo, Japan)
- Since 2020-07 Professor, by courtesy, Goethe University Frankfurt at the Faculty of Computer Science and Mathematics (FB12)

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

	SS 2024	WS 2024/2025
Bachelor		*Course* **Business Informatics 2 (PWIN)**
Master	*Course* **Mobile Business II:** **Application Design, Applications, Infrastructures and Security** *Course* **Information and Communication Security: Infrastructures, Technologies and Business Models** *Course* **Privacy vs. Data:** **Business Models in the digital, mobile Economy** *Seminar* **The Future is Now: Topics with and about ChatGPT and AI**	*Course* **Mobile Business I:** **Application Design, Applications, Infrastructures and Security** *Course* **Information and Communication Security: Infrastructures, Technologies and Business Models** *Seminar* **Machine Learning: Privacy, Regulations and Ethical Issues**

Teaching in Frankfurt

Teaching Topics

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

Master Courses

Lectures

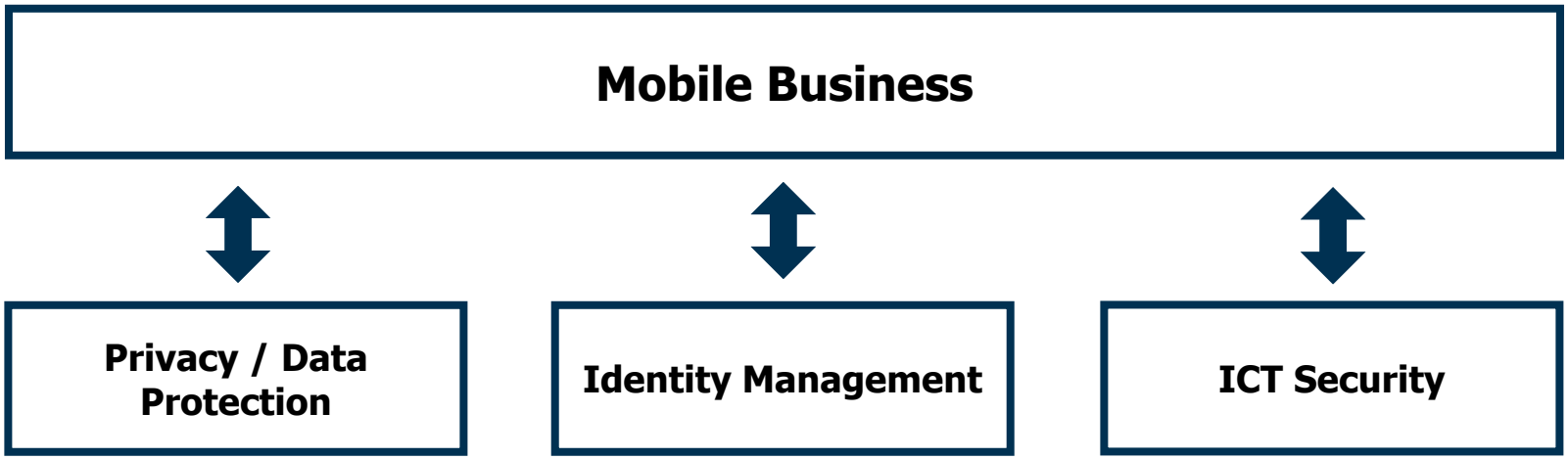
- Mobile Business 1
- Mobile Business 2
- I & C Security
- Privacy vs. Data
- Seminars
- Master Thesis

Bachelor Courses

Lectures

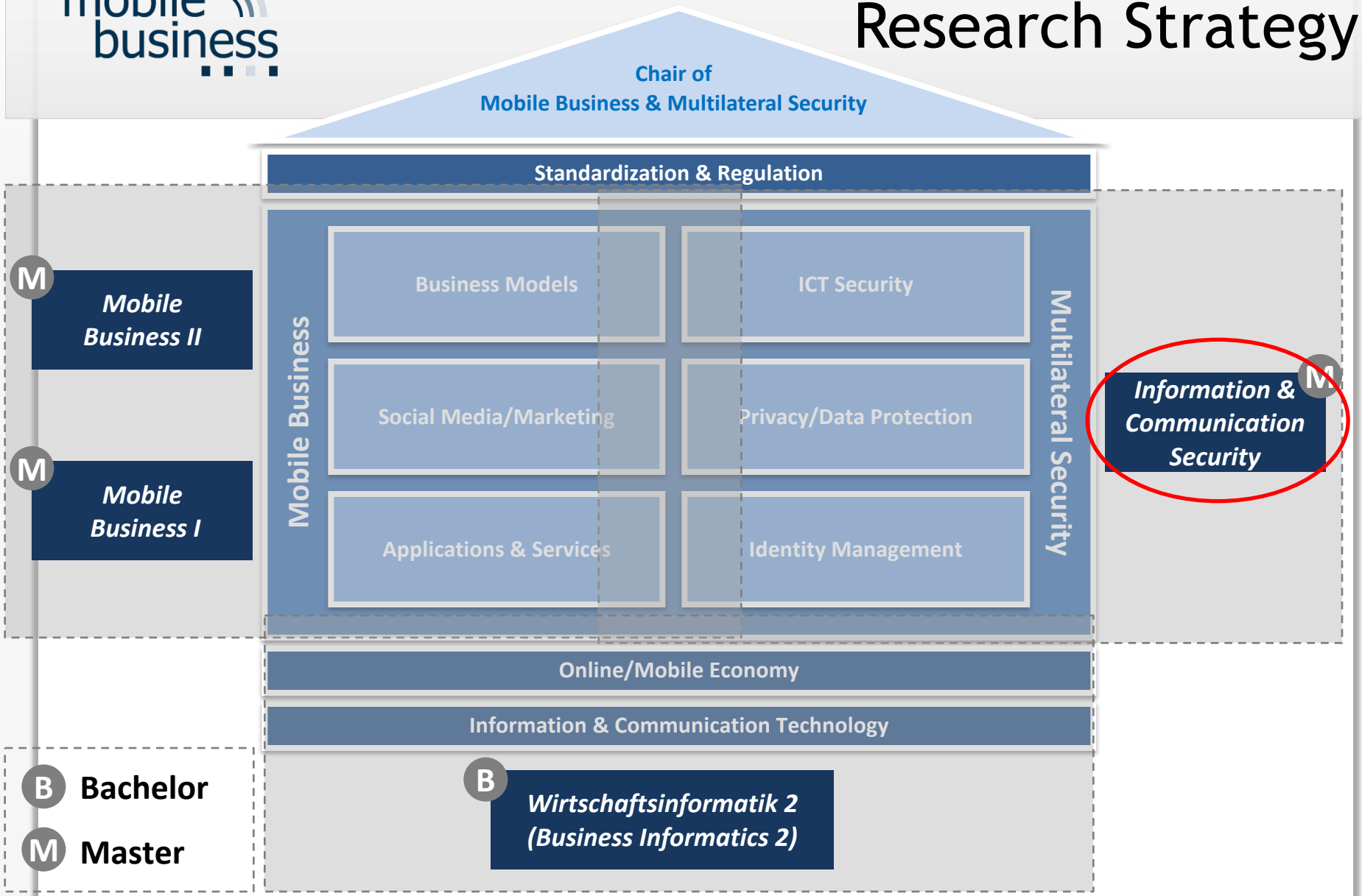
- Business Informatics 2
- Seminars
- Bachelor Thesis

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
  - Security and Privacy Management
  - 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

Teaching Assistance

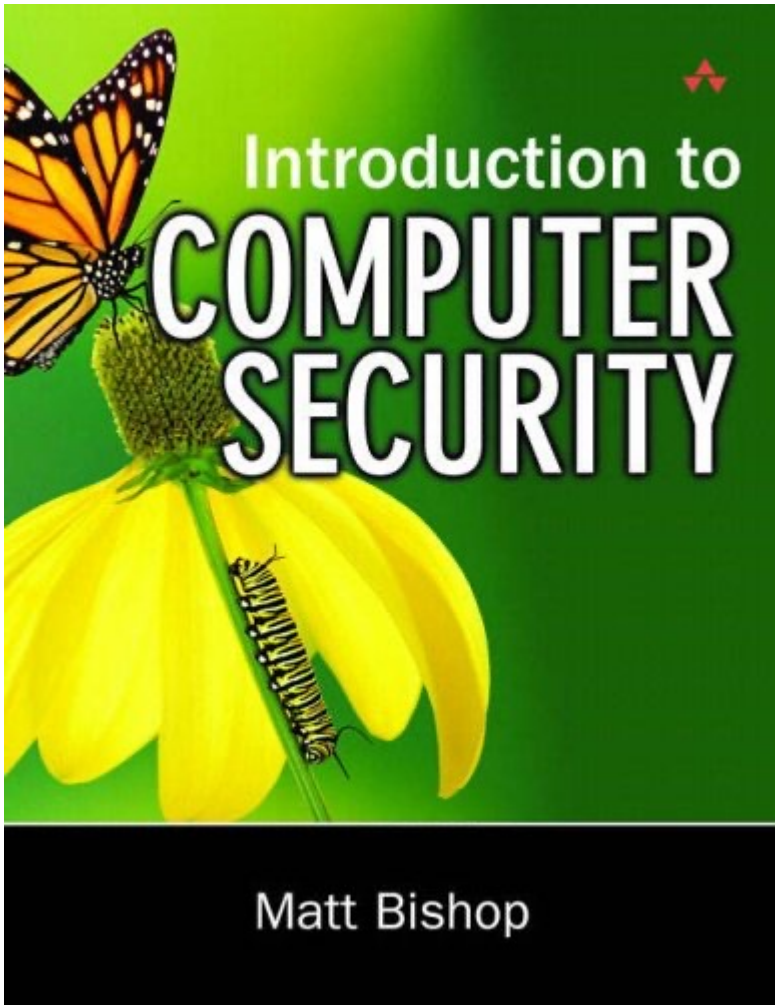
Sascha Löbner, M.Sc.

RuW Building, Office 2.236

Email: sascha.loebner@m-chair.de

security@m-chair.de

Literature



Matt Bishop:

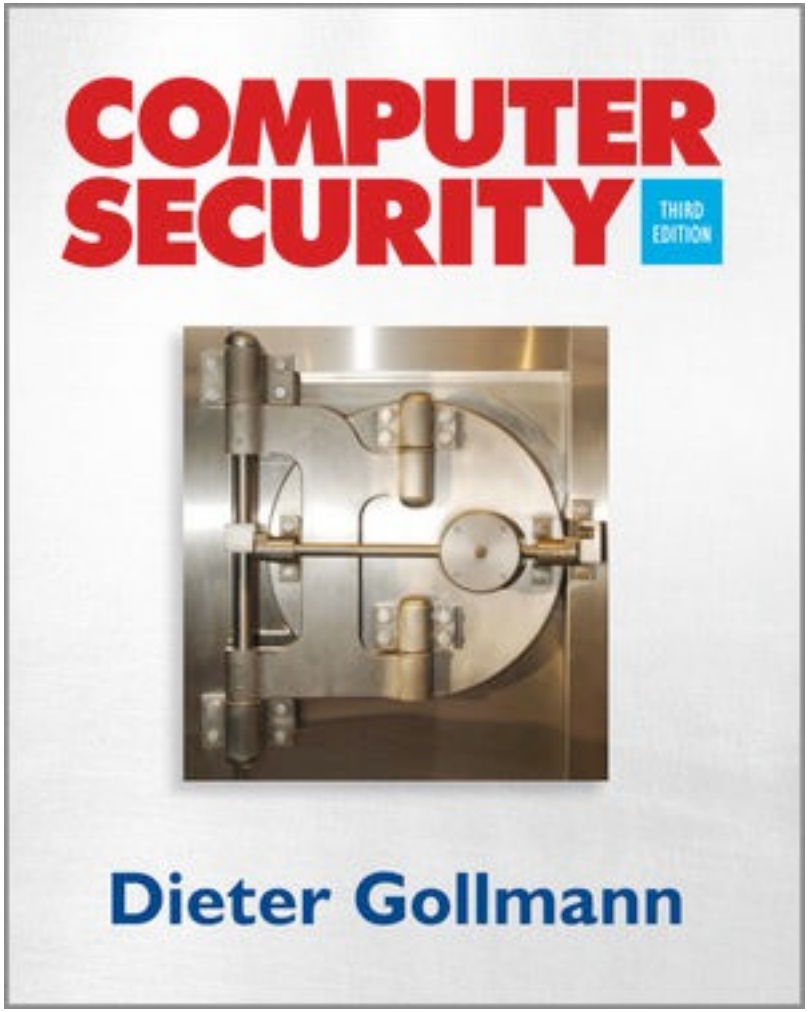
Introduction to Computer Security

Addison Wesley

ISBN: 0-321-24744-2

mobile business

Literature



Dieter Gollmann:

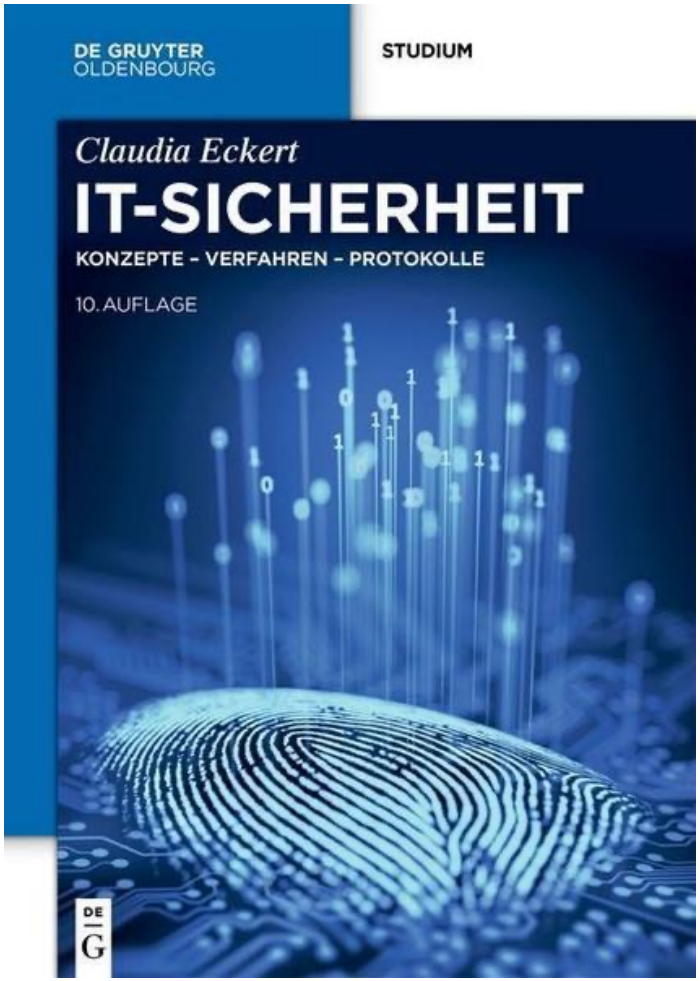
Computer Security

John Wiley & Sons

ISBN: 0-470-74115-5

19

Literature



In German:

Claudia Eckert:

IT-Sicherheit

Oldenbourg

ISBN: 978-3-11-055158-7

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

EBSCO HOST Research Databases

Internet search engines:

academic.live.com
scholar.google.com

21

On the dates and the agenda

- **Exam date and regulations not fixed yet.**
  - Please keep yourself updated!
  - Check the website of the examination office:

  https://www.wiwi.uni-frankfurt.de/en/study/services/examination-office/service-and-contact.html
- **Course agenda is online.**
  - Please keep yourself updated!
  - Check the website of the course:

  https://www.m-chair.de/index.php?option=com_teaching&view=lecture&id=67

Agenda

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

Electronic Business and Security

The New York Times

Facebook Security Breach Exposes Accounts of 50 Million Users

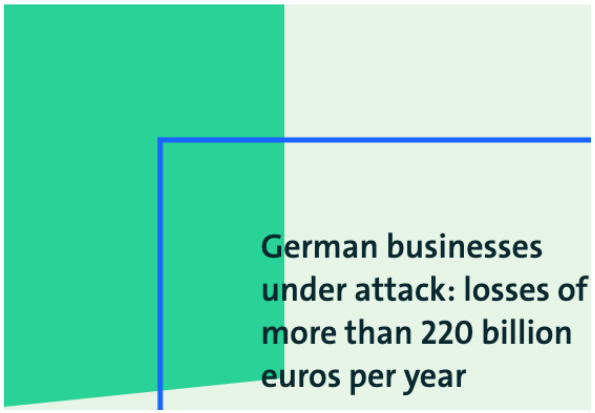
Sept. 28, 2018

February 15, 2012, 2:14PM

Anonymous-Linked Attacks Hit US Stock Exchanges

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

bitkom



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

The New York Times

Security Gap Leaves 885 Million Mortgage Documents Exposed

May 24, 2019

BBC Sign in | News | Sport | Reel | Worklife | Travel | Future | More

NEWS

Facebook's Twitter and Instagram accounts hacked

8 February 2020

Risks of Unprotected Market Activities

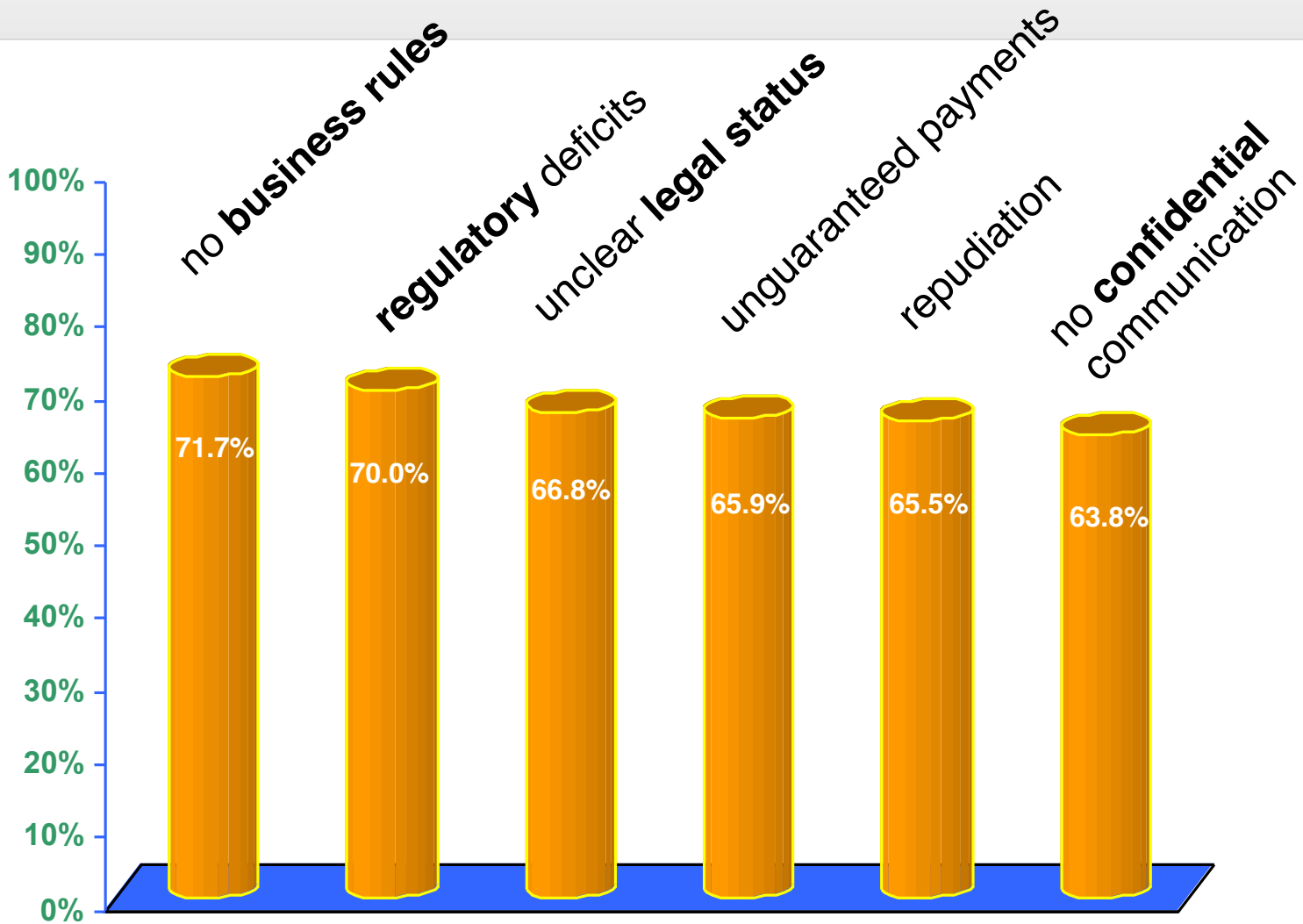
Provider

- No payment – debtor cannot be captured
- Wrong or fake orders
- Copyright violations
- www attacks
- Internal server intrusion
- …

Consumer

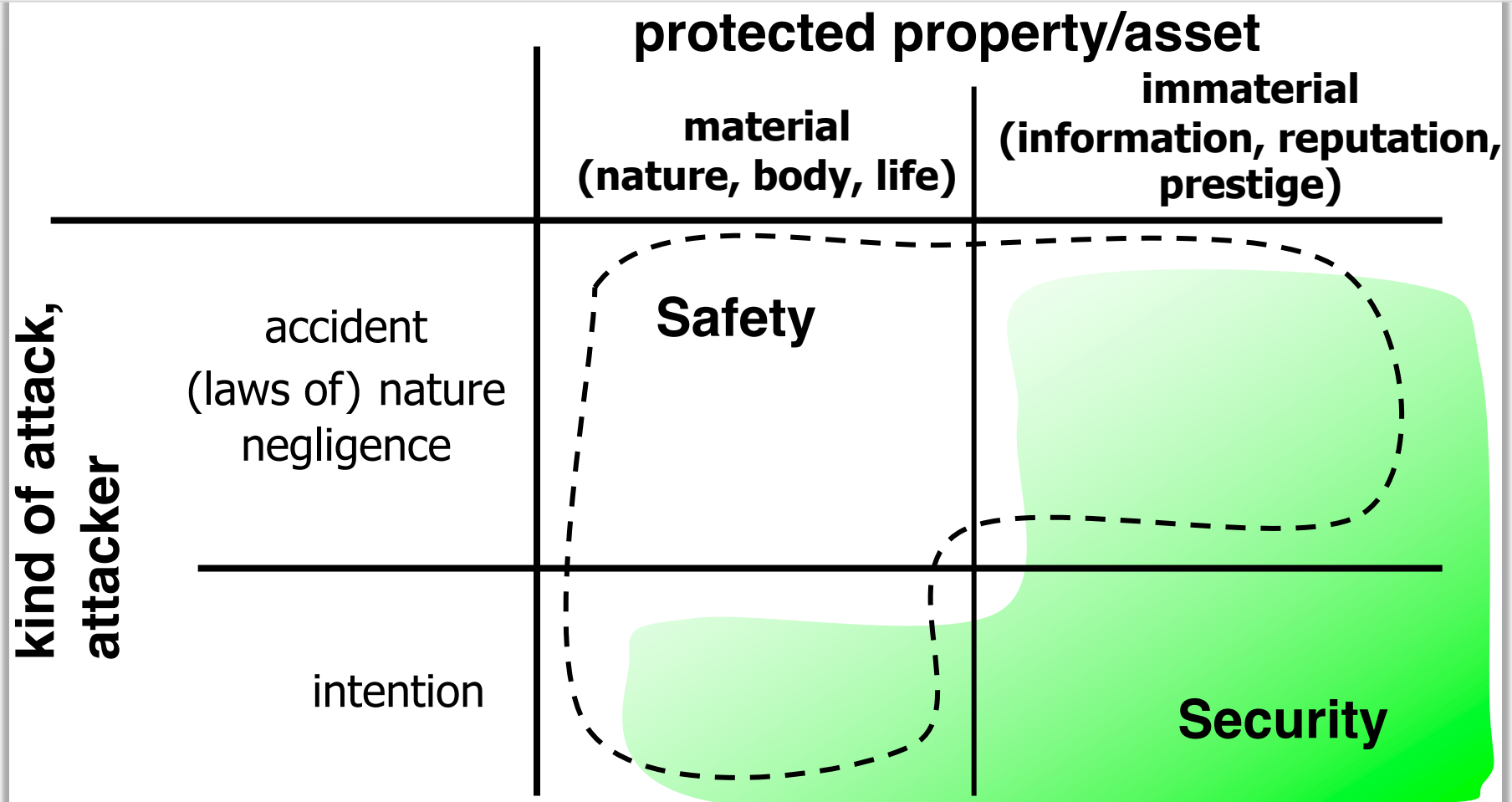
- Unwanted deliveries (false, not ordered, …)
- Unauthorized / unexpected direct debt of money, e.g. from a credit card account
- Unwanted advertising mail (“spamming”)
- Transparent consumers
- …

E-Commerce Requires Security



Source: Electronic Commerce Enquête, Universität Freiburg, 1998 [Schoder, Müller 1999]
(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

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. [Rannenberg 2000a]

Confidentiality

- ***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.

Integrity

- ***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 creates 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.

mobile business

Availability

- ***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.

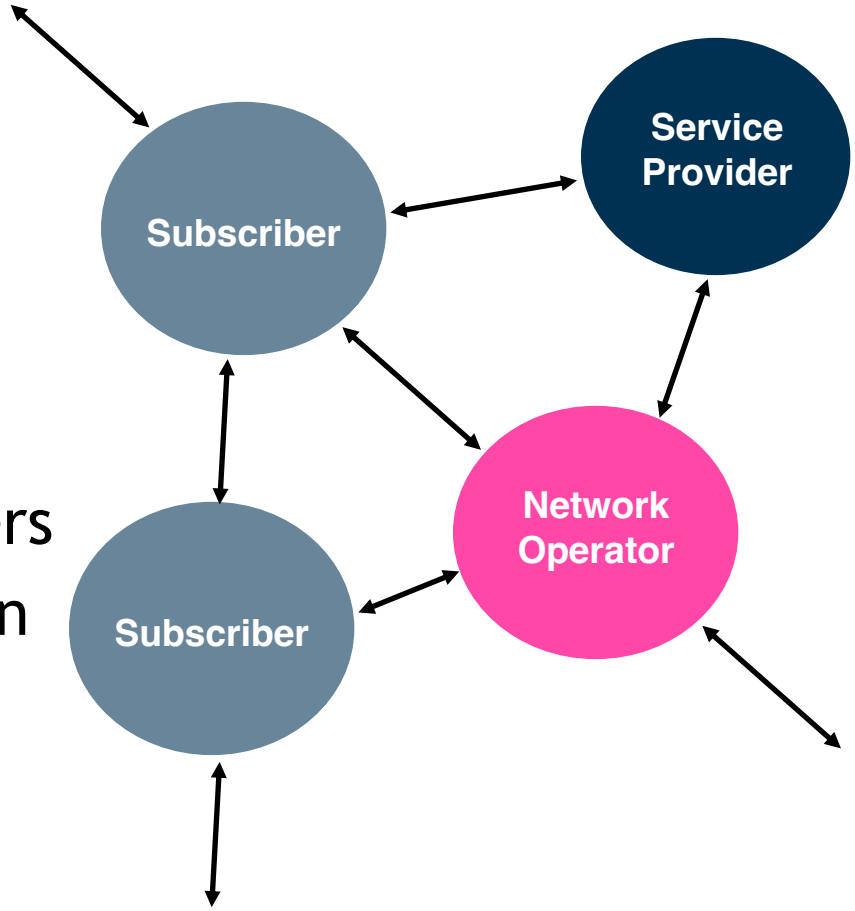
Accountability

- ***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, unresponsible 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.

Multilateral Security

Different Parties
with
different Interests

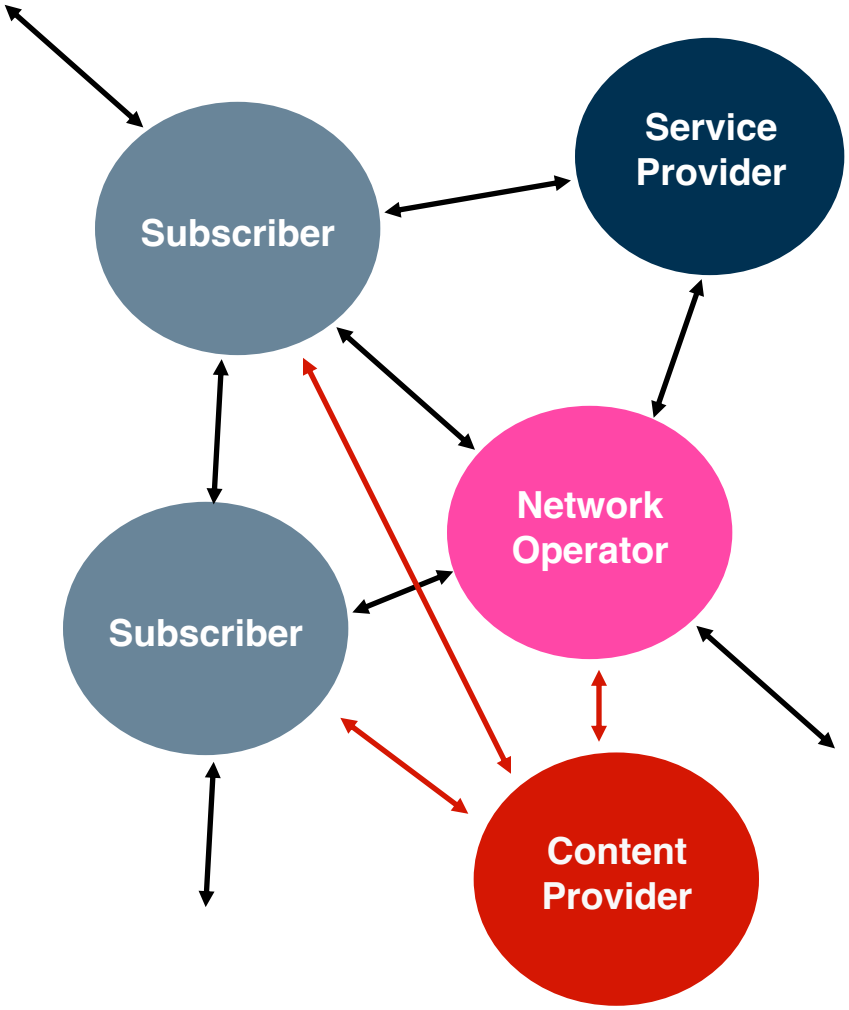
- Customers/Merchants
- Communication partners
- Citizens/Administration



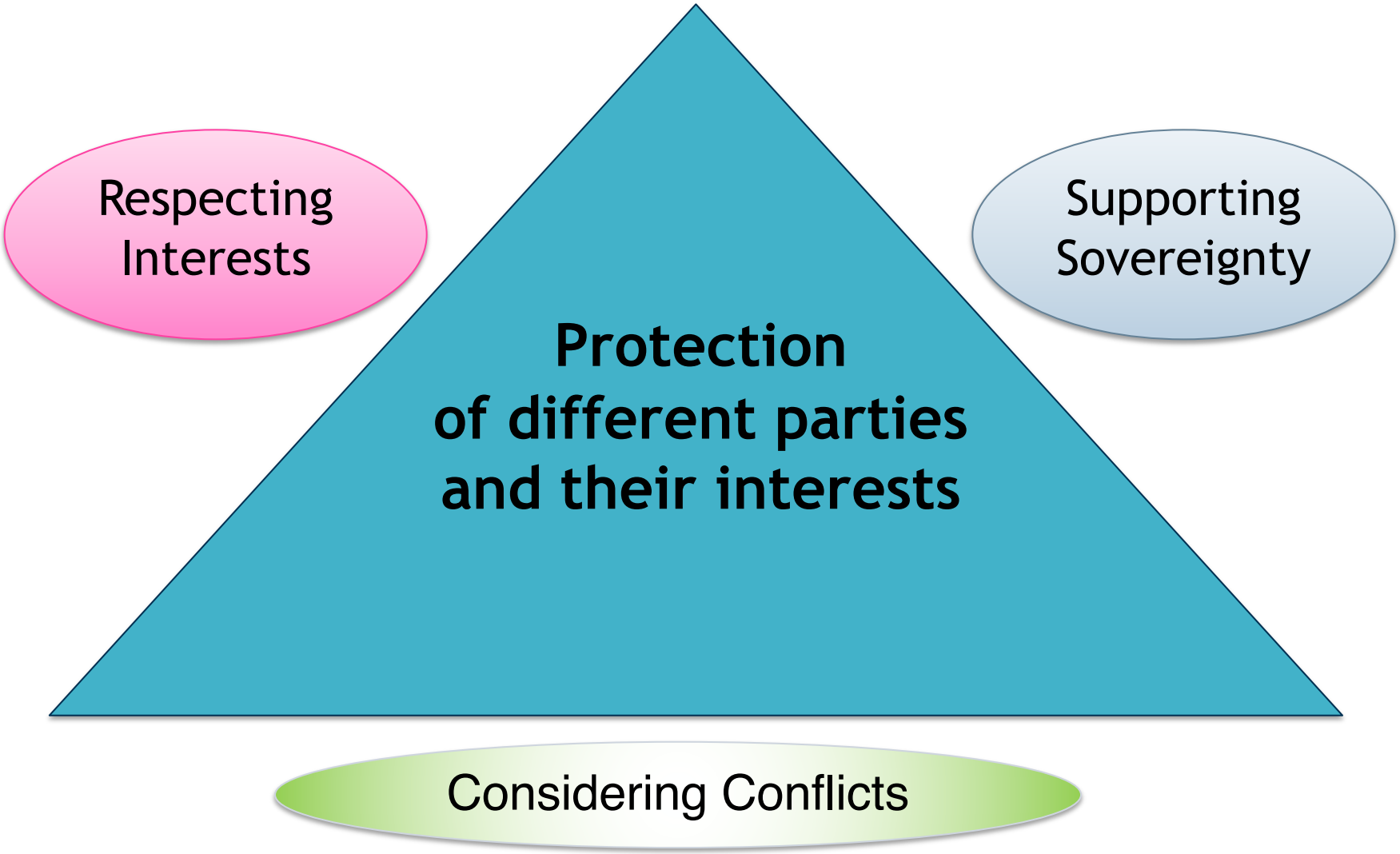
Multilateral Security

… 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

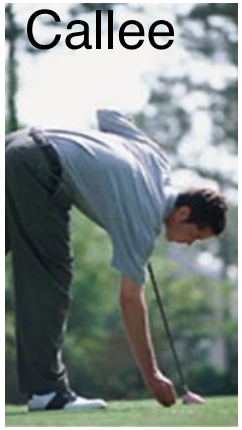
→ Reachability Management (RM)

[Rannenberg 2000b,c]

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



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!"

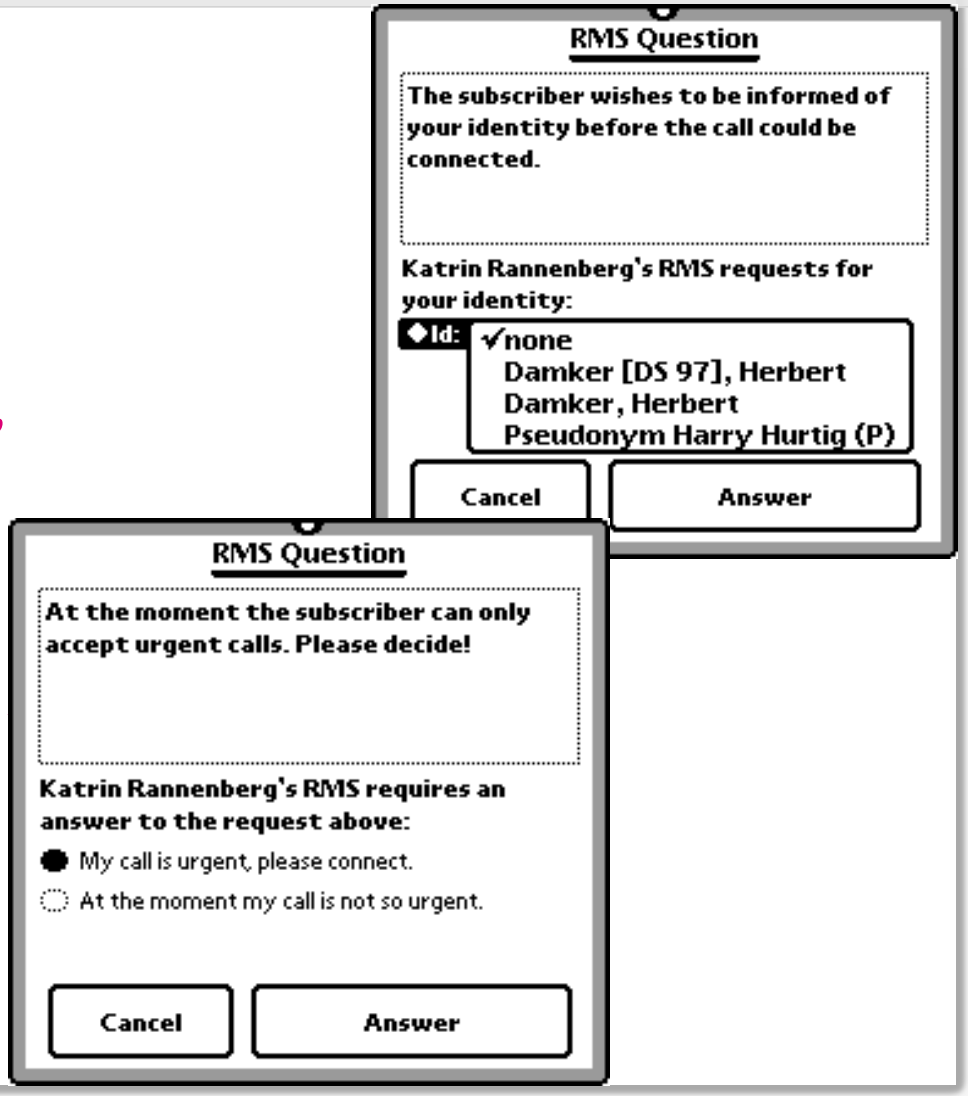
Specification of a function
"I am your boss!"

Specification of a subject
"Let's have a party tonight."

Presentation of a voucher
"I welcome you calling back.

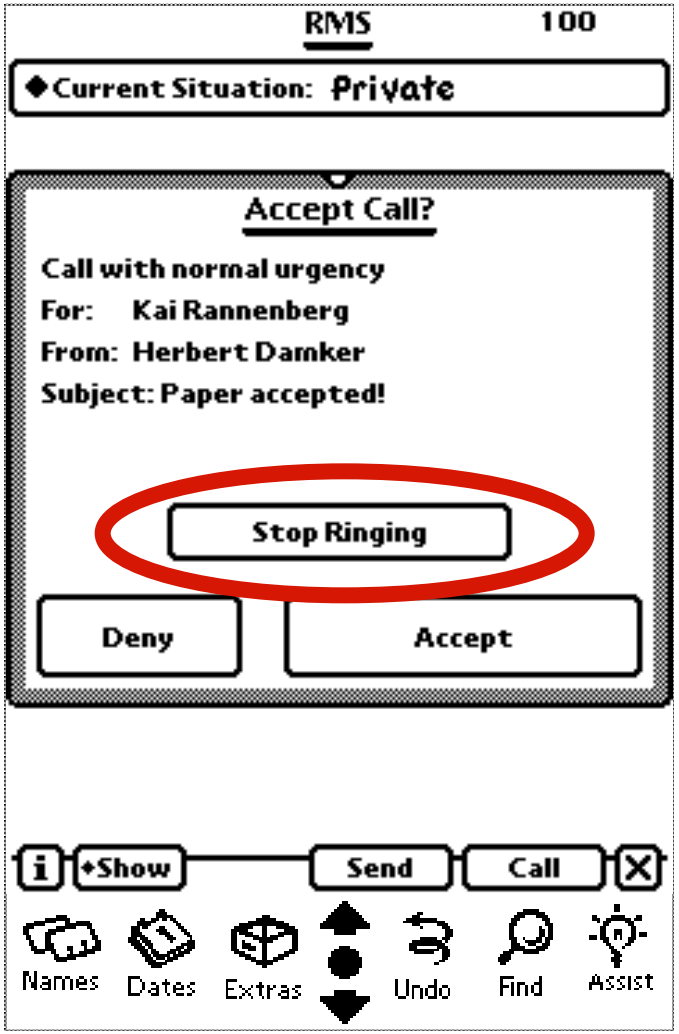
Provision of a reference
"My friends are your friends!

Offering a surety
"Satisfaction guaranteed
or this money is yours!"



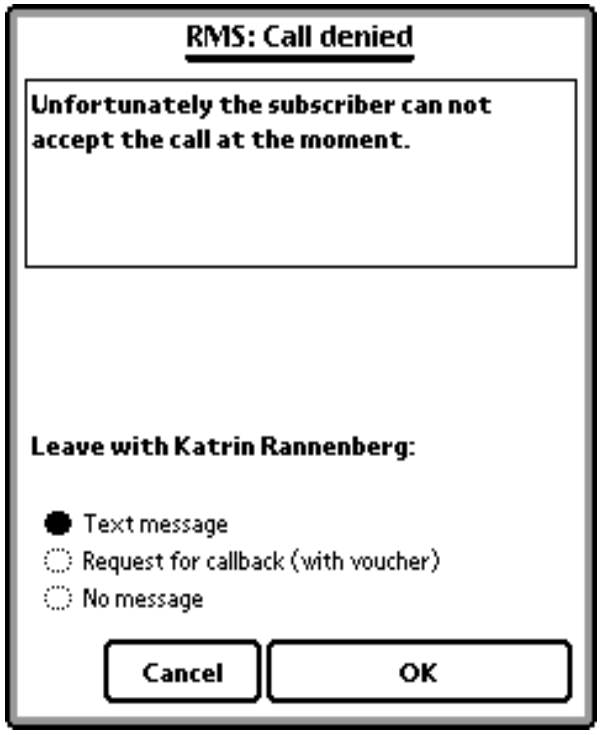
RMS accepted call (Callee display)

- 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

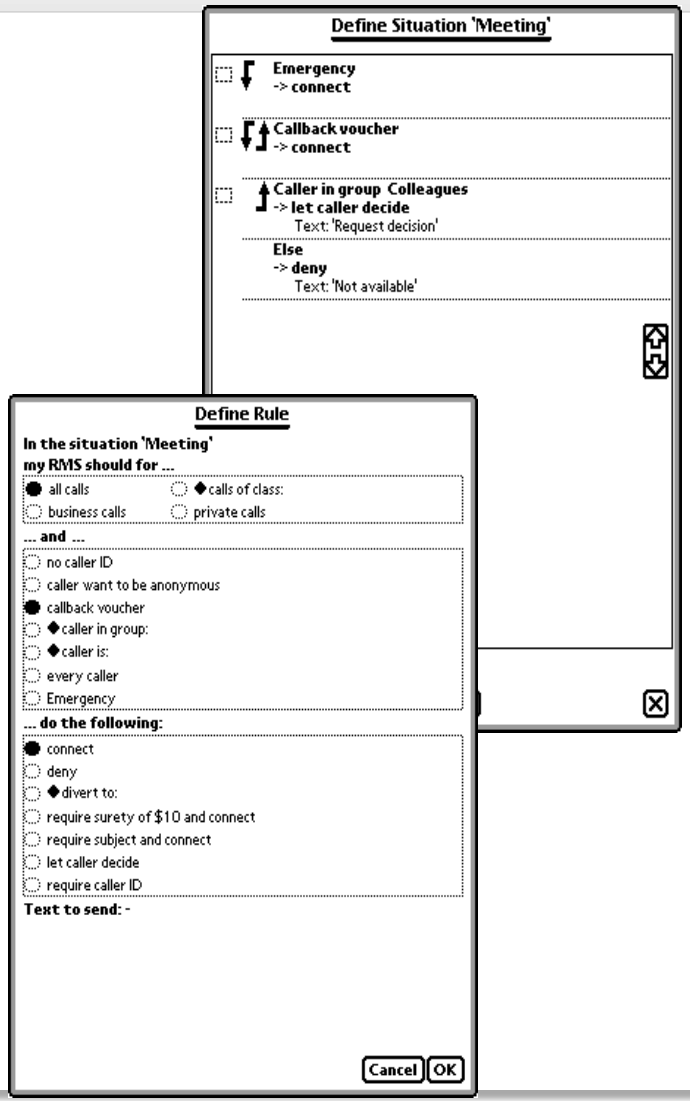
Situations

Set of rules how to deal with an incoming call

Rules

Combination of features

Users can reconfigure initial rules and situations as they like.



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

References

- [FGGKMMRS 2014] Felix Freiling, Rüdiger Grimm, Karl-Erwin Großpietsch, Hubert B. Keller, Jürgen Mottok, Isabel Münch, Kai Rannenberg & Francesca Saglietti: Technische Sicherheit und Informationssicherheit, Unterschiede und Gemeinsamkeiten; Informatik-Spektrum, February 2014, Vol. 37, Issue 1, February 2014, pp. 14-24, DOI: 10.1007/s00287-013-0748-2; https://fb-sicherheit.gi.de/fileadmin/FB/SICHERHEIT/AKBegriffsbildungIS-1-2014.pdf
- [Rannenberg 2000a] Kai Rannenberg: Mehrseitige Sicherheit - Schutz für Unternehmen und ihre Partner im Internet; Wirtschaftsinformatik Volume 42, pp. 489-497 (2000), https://link.springer.com/article/10.1007/BF03250765
- [Rannenberg 2000b] Kai Rannenberg: Multilateral Security – A concept and examples for balanced security, pp. 151-162 in Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3, https://m-chair.de/images/documents/publications/Rannenberg/p151-rannenberg.pdf
- [Rannenberg 2000c] Kai Rannenberg: How much negotiation and detail can users handle?, pp. 37-54 in Frédéric Cuppens et al.: Computer security: Proceedings of the 6th European Symposium on Research in Computer Security; October 4-6, 2000, Toulouse, France; Lecture Notes in Computer Science 1895, Springer-Verlag; ISBN 3-540-41031-7, https://m-chair.de/images/documents/publications/Rannenberg/ESORICS-f-1.7.mh.pdf
- [Schoder, Müller 1999] Detlef Schoder, Günter Müller: Potentiale und Hürden des Electronic Commerce – Eine Momentaufnahme, Informatik-Spektrum Volume 22, pp. 252–260 (1999), https://link.springer.com/article/10.1007/s002870050142