Network Security (NetSec)

Summer 2015
Chapter 00: Organization & Introduction
Module 01: Organization of the Lecture

Image source: http://banksystreetart.tumblr.com/

Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Overview of this Module

(1) The NetSec team welcomes you
(2) Philosophy of the lecture
(3) Objectives of the lecture
(4) Orga … locations, dates, administration
(5) Other related courses at SEEMOO

Chapter 00, Module 02

Welcome

Welcome

SECURE MOBILE NETWORKING

Prankur Chauhan

Dennis Giese

Milan Schmittner

Matthias Hollick

Marc Werner

Johny George Malayil

N.N. - Gastsprecher

The NetSec Team – Welcome

Matthias Hollick

- Building S4/14, Room 4.2.07 – 4.2.09
- mhollick@seemoo.tu-darmstadt.de
- http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Short CV

- 2009 Professor for Secure Mobile Networking at TU Darmstadt
- 2009 Associate Professor at Universidad Carlos III de Madrid
- 2007 Research Scholar at University of Illinois at Urbana-Champaign
- 2004 PhD in ETIT from TU Darmstadt

Research area

- QoS, Security, Privacy in Wireless (Multihop) Networks
- Secure Mobile Computing/Mobile Networking in general

The NetSec Team – Welcome

SECURE MOBILE NETWORKING

Pierre-Louis Cayrel

- S4/14, 5.3.28
- pierre-louis.cayrel@cased.de

Short CV

- Since 2009 PostDoc at CASED in the area of Crypto
- 2008 PhD in Mathematics from Université de Limoges

Research area

- Code-based Cryptography

André König

- S3/20, 203
- andre.koenig@kom.tu-darmstadt.de

Short CV

- 2010 PhD in ETiT, TU Darmstadt
- Since 2005 Research Assistant at KOM, TU Darmstadt

Research area

- Security in Distributed and Dezentralized Systems & the Future Internet

The NetSec Team – Welcome

WiMis

- Milan Schmittner
  - The main contact w.r.t. all organizational issues
  - Researches on Networks for Emergency Response & Security
- Marc Werner
  - Backing up Milan, researches on Wireless Mesh Networks

Tutors

- Prankur Chauhan
- Dennis Giese
- Johny George Malayil

Guests

- We are planning for guest lectures, but not all topics are confirmed

Philosophy & Objectives

Lecture Philosophy

Scope of the course: security in communication networks

- Characteristics, principles, problems, peculiarities, and effects
  - How to and how not to approach problems
- Broad (plethora of security fundamentals & technologies)
  - Covers all layers from physical to application: commonalities, strengths, weaknesses, practical aspects
- But also deep
  - Emphasis on Internet security, hands-on for selected topics

Approach:

- Learning from existing systems (principles, protocols, and practice)
  - Transfer fundamentals of IT security and crypto to networks
  - Top-down approach to network security (from APP to PHY)
- Discuss state of the art in technology and current research problems

Learning Objectives

As taken from the TUCaN description

- "*Students attending the lecture are acquiring knowledge in the domain of communication network security with emphasis on Internet security. Students are able to apply and transfer the most important fundamentals from IT security and cryptography to the field of communication networks.*"
- "*Students … have a thorough understanding of security mechanisms on the different network layers (application layer, transport layer, network layer, link layer, physical layer). As a result, they are able to thoroughly discuss the characteristics and principles in the area of network security and exhibit detailed theoretical and practical knowledge in this field. Additionally, students are able to describe recent developments in the area of network security (e.g. peer-to-peer security, mobile network security, etc.).*"
- "*The exercise deepens the theoretical foundations by means of exercises, which consist of literature, calculation as well as practical implementation/application examples.*"

How to fail this course

Source: http://www.leadernetworks.com/

General Remarks

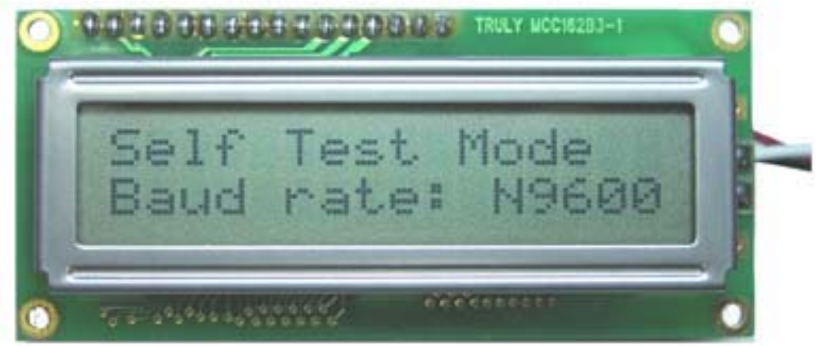
How to fail NETSEC lecture

(1) Laziness (or overbooking your schedule)
(2) Missing prerequisites in either networking or IT security
(3) Choosing NETSEC solely because it is in english
(4) A combination of the above

A Cautious Note

Please note, last year we had severe problems with students of who underestimated this course!

We will offer a concise self-test on the learning platform to help you assessing if you meet the prerequisites. Take this seriously, particularly, if you did not do the Bachelor at TU Darmstadt.



Source: www.imagesco.com

If you are missing prerequisites there are still many options:

- You can build the necessary background … we will offer NetSec 2016
- You can self-study if you are missing only small parts … there are excellent textbook on networking, crypto, IT-security (but be aware that this takes additional time)

Dept. of Computer Science | SEEMOO | Prof. Dr.-Ing. Matthias Hollick

Organization

Organizational Issues (1)

Course mode

- Integrated course, 6 ECTS credits
- Exercises schedule can be found on learning platform
- The course is offered in the summer term

Course language is English

Time and location for lecture & exercise

- On Wednesdays, from 13:30 to 15:10h, room S202/C205
- On Thursdays, from 9:50 to 11:30h, room S202/C205

We offer recordings via our learning platform … either freshly recorded or from the past, if the contents have not changed

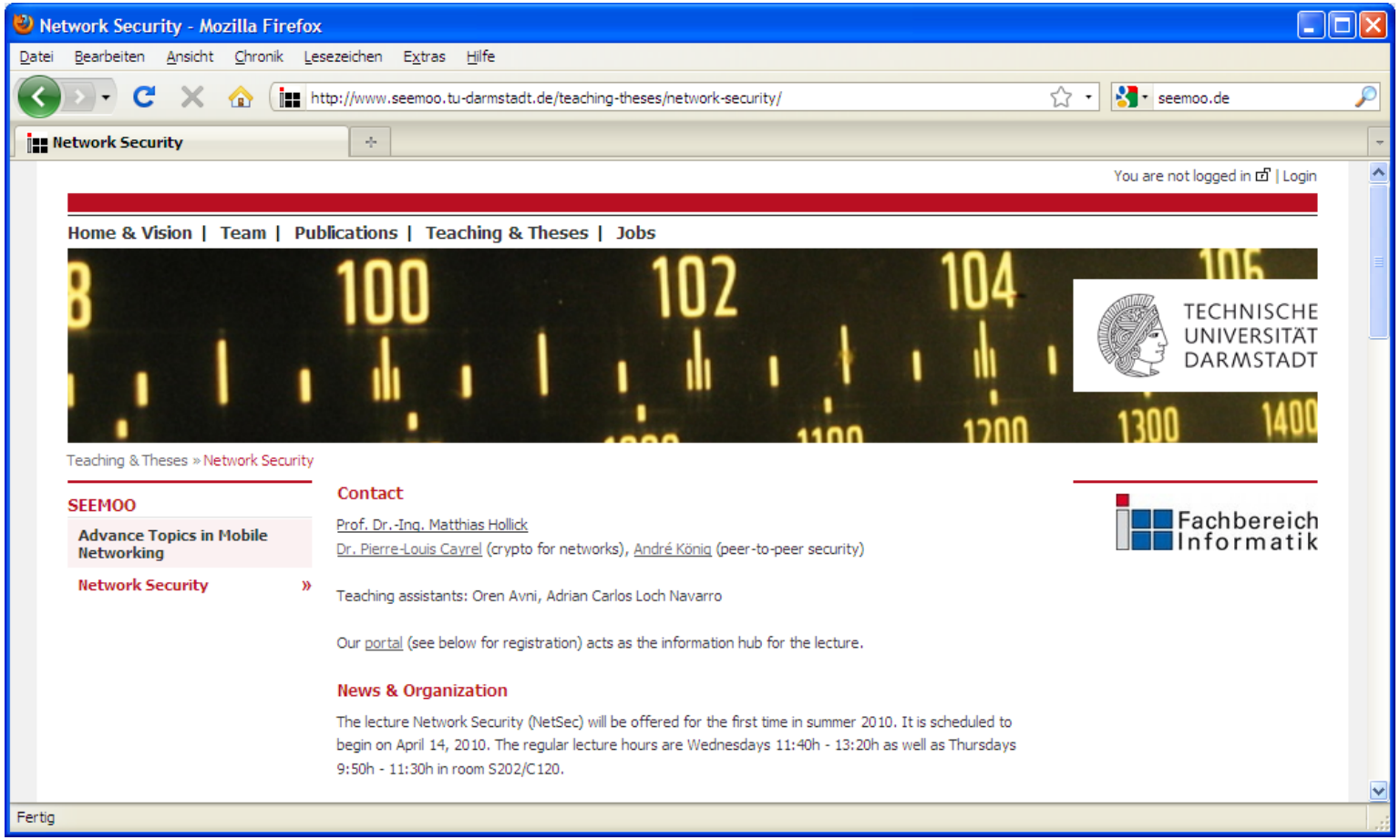
Organizational Issues (2)

Prerequisites

- Basic courses of Bachelor are required
- Knowledge in the areas
  - IT Security,
  - Introduction to Cryptography, and
  - Communication Networks is required
- Keen interest to explore challenging topics which are cutting edge in technology and research
- Only your exam office can tell you, if this lecture fits your study plan
  - If you have difficulties convincing your exam office that NetSec is the greatest thing since sliced bread, please let me know!

Organizational Issues (3)

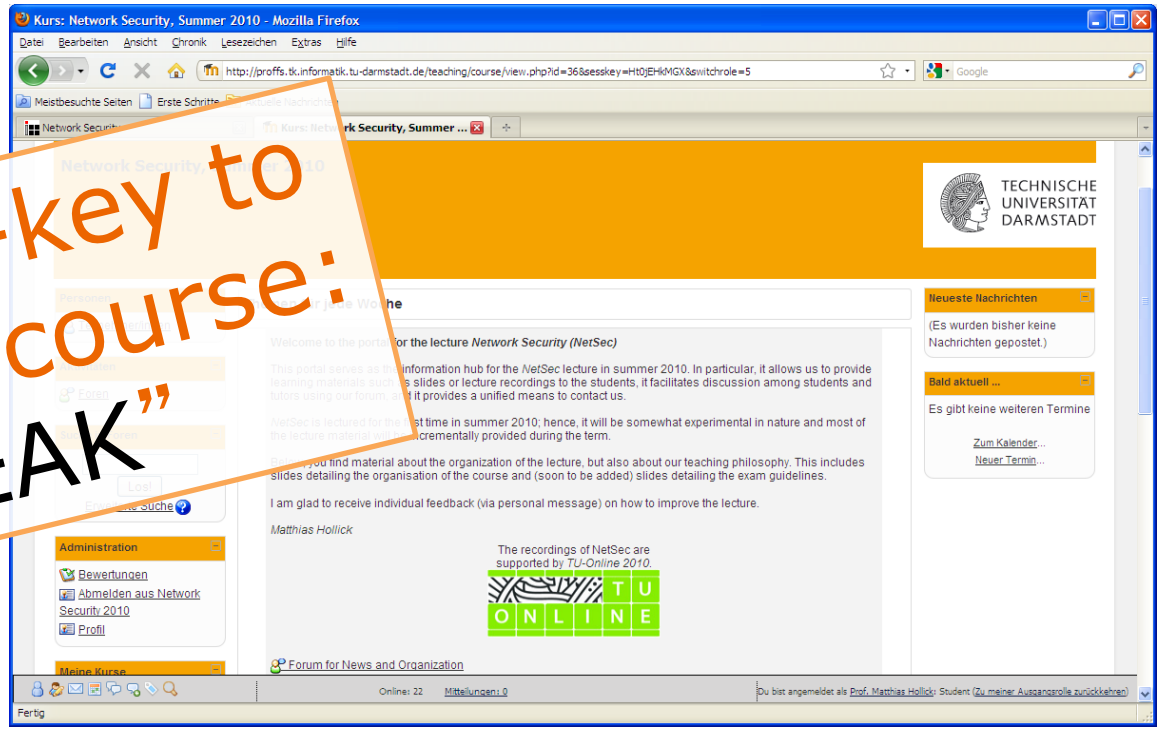
"Static" course infos are available at https://seemoo.de/teach



Organizational Issues (4)

"Dynamic" course infos are available at our course portal Moodle

- https://moodle.informatik.tu-darmstadt.de
- With your TU-ID, you can register for he course. See also info on https://seemoo.de/netsec/



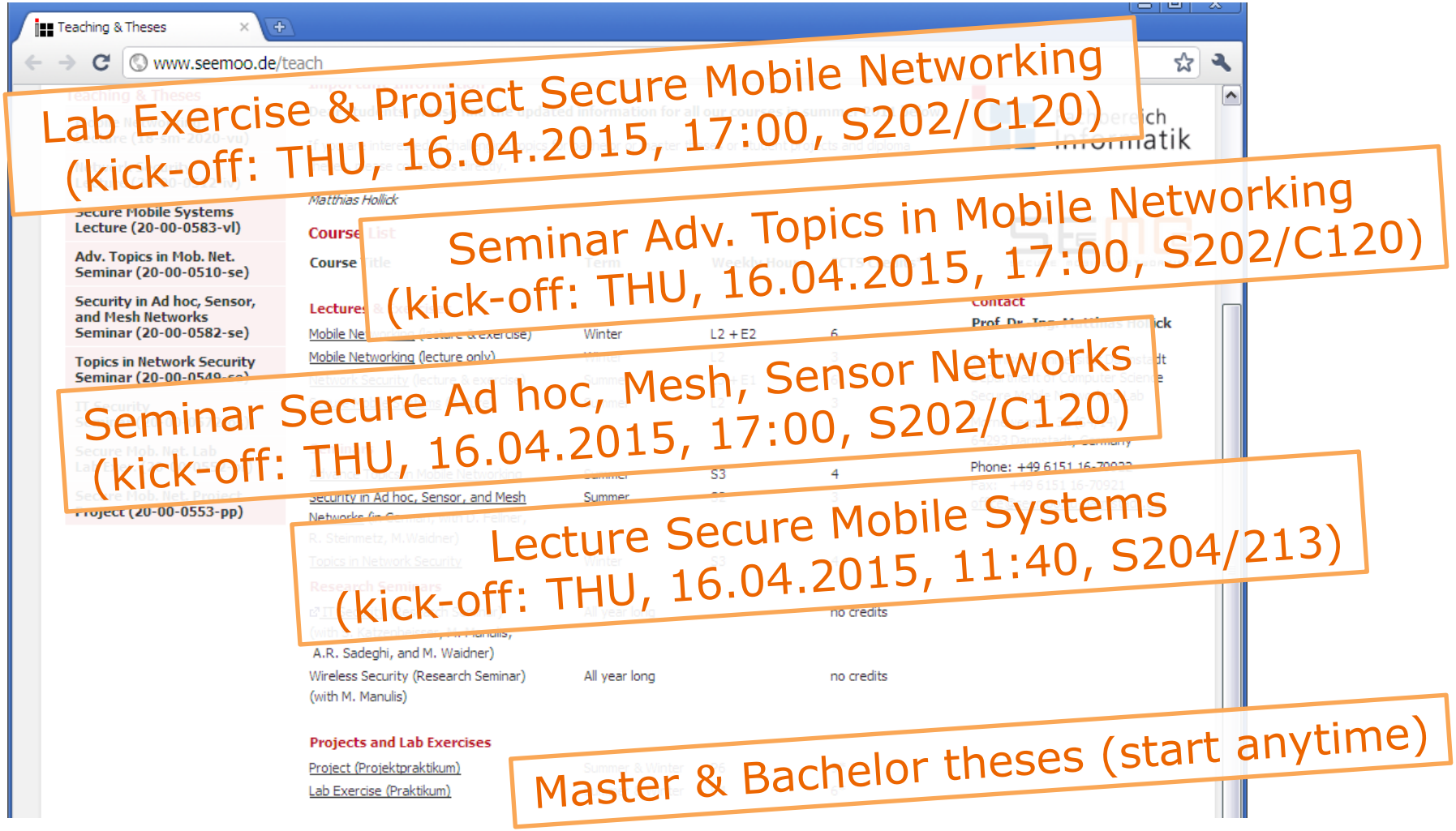
One-time-key to enter the course: "FREAK"

Bonus?!

We decided to honor students that are active and contribute to the lecture (sort of motivating you to self-motivate)

Details in the next module …

Related courses at SEEMOO



Related courses at SEEMOO

Related courses at SEEMOO

Lecture “Simulation & Modelling in Mobile Networks”

Objectives of this lecture

- Understanding basics of simulations, application of statistics to simulations
- Developing and understanding simulation environments for mobile networks
- Application of theoretical knowledge to practically motivated setups

Modus Operandi

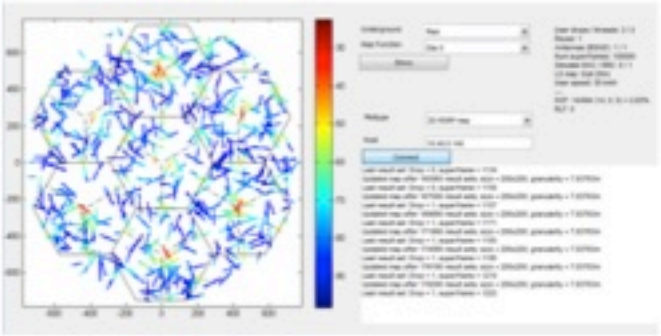
- Three parts:
  - 1/3: Theoretical concepts of simulations
  - 1/3: Simulation environments for mobile networks
  - 1/3: Discussion based on simulation example
- Targeted audience: Masters Students
- Prerequisites: Communication Technology, Communication Networks, Signal Processing
- Timing
  - Based on feedback of students: block lecture at the begin, mid, or end of semester
- Oral exam
- 3 Credit Points

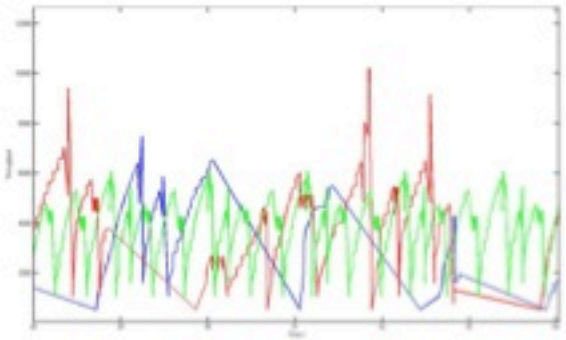
Lecturers: Dr. Peter Rost, Dr. Andreas Maeder (NEC Labs Europe, Heidelberg)

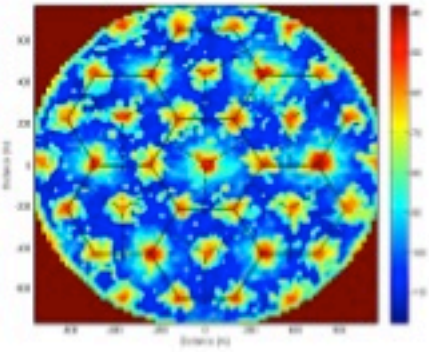
General

Outline

- Part I: Introduction
- Part II: Basics of probability theory, stochastics, simulators
- Part III:
  - Mobile communications systems (basics, standards)
  - Link-Level simulations (basics, tools, example)
  - System-Level simulations (basics, tools, example)
  - Packet-Level simulations (basics, tools, example)







Info session

An information session for the projected lecture will take place on

April 15th 2014, 13:30 h in S3 06/room 052.

All interested students are requested to attend!

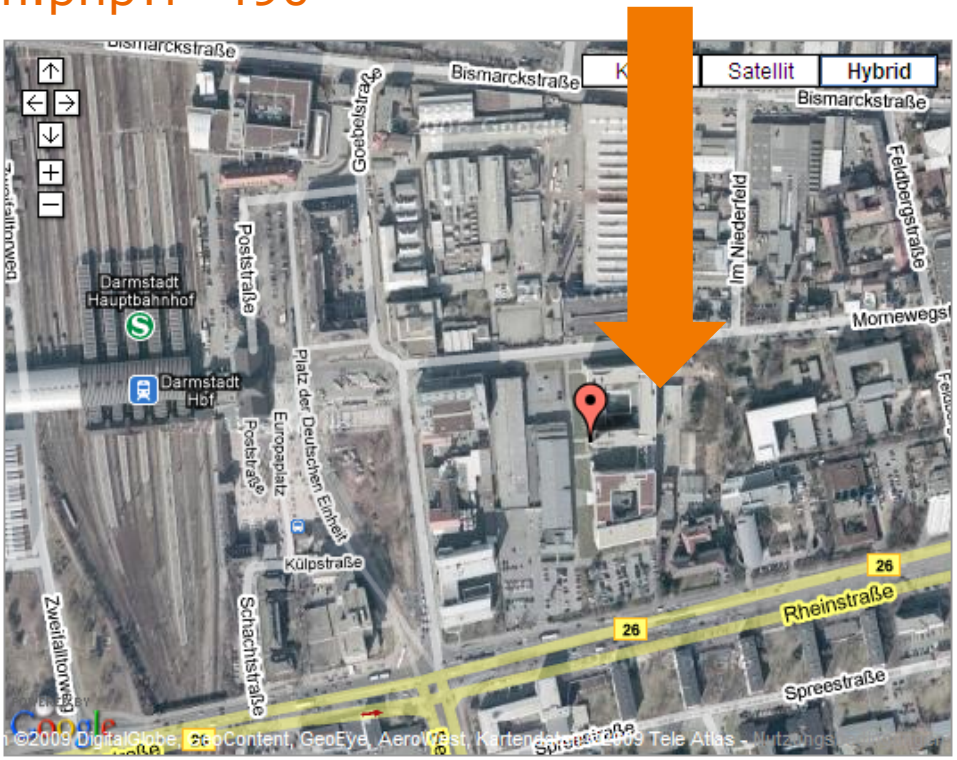
Contact Us

All questions relevant for lecture, exercise, organisation

- Forums within our learning portal Moodle
- Forum of FS Informatik exists, but we do not regularly monitor it
  http://d120.de/forum/viewforum.php?f=490

Or contact us in the real-world

- Building S4/14
  Room 4.2.07 & 4.2.09
  Mornewegstr. 32
  64293 Darmstadt
- Consultation hours:
  Friday 14:00-15:00
  (but confirm by email
  mschmittner
  @seemoo.tu-darmstadt.de)



Advertisement – Girls Only

Pick up a flyer to get more info! We will fund scholarships.
GHC will take place in Phoenix, Arizona, Oct 8th – Oct 11th.

MAKI-Wettbewerb für Studentinnen

der Fachbereiche 18 und 20 um die Teilnahme an

Grace Hopper Celebration of Women in Computing

Sie sind Studentin der Elektrotechnik und Informationstechnik oder der Informatik?

Sie sind in ihrem Fach besonders engagiert und erbringen gute Studienleistungen?

Sie interessieren sich für internationale Karrierewege?

ANITA BORG INSTITUTE
GRACE HOPPER
CELEBRATION OF WOMEN IN COMPUTING

Advertisement – Eve

Tomorrow!

Prof. Fred Schneider

"Toward a Science of Security"

Cornell University, Department of Computer Science, USA

Attention! New location: Piloty Building, S2 | 02, room C 205

April 24, 2014, 4:15-5:15 p.m.

Abstract:

While today much security research is about defending against the attack du jour, there has been theoretical work in computer security and there are the beginnings of a science base for security. This talk will discuss the kinds of questions one might expect a scince base to address.

It will also give examples of how such questions could be answered. Basic concepts in security, such as attack, policy, and enforcement turn out to be surprisingly subtle to define.

Continue

Further information on Prof. Fred Schneider

SFB 1053 MAKI

TECHNISCHE UNIVERSITÄT DARMSTADT

Distinguished Lecture Series Summer 2014

www.maki.tu-darmstadt.de

Bringing leading researchers to TU Darmstadt to promote the exchange of thoughts and ideas between the speakers, students, faculty and the public on the latest advances in the area of networked communication systems and the future internet

Thomas Wiegand

Fraunhofer HHI & TU Berlin, Germany

Mai 15, 2014
S2-02/C110 16:15h

Recent Advances in Video Communication

Thomas is one of the fathers to the standard that today compresses the majority of video bits: H.264/MPEG-AVC. His research is on efficient compression and transmission of video, including scalable coding, high definition and 3D video coding and video-adaptive network coding.

Thomas received his Dr.-Ing. from the University of Erlangen-Nuremberg in 2000 and worked at Heinrich Hertz Institute HHI (Germany), Kobe University (Japan), UCSB and Stanford (US). Currently, he is a Professor in the EE/CS Dept. of TU Berlin, where he chairs the Image Communication Laboratory. He is jointly heading the Fraunhofer HHI, Berlin, Germany.

Jörg Widmer

IMDEA Networks Madrid, Spain

June 5, 2014
S2-02/C110 16:15h

Design Considerations for 60 GHz Wireless Networks

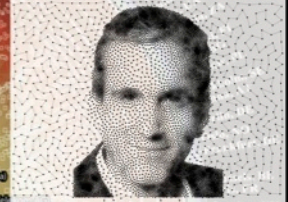
Jörg's research focuses primarily on wireless networks, ranging from MAC layer design and interference management to future mobile network architectures. Current work includes extremely high frequency communication (60GHz) as well as network coding for wireless networks.

Jörg earned his doctoral degree from the University of Mannheim in 2003. He worked at EPFL (Switzerland) as well as DoCoMo Euro-Labs (Germany). He was a visiting researcher at ICSI (Berkeley, CA, US) and the University College London (UK). Jörg is currently a Research Professor at Institute IMDEA Networks, Madrid, Spain.

Edward Knightly

Rice University Houston, United States

June 12, 2014
S2-02/C110 16:15h



Diverse Spectrum Multi-User MIMO: from WLANs to Urban Access

Edward's research interests are in the area of mobile and wireless networks with a focus on protocol design, performance evaluation, and at-scale field trials in urban wireless networks. His group contributed to key features of IEEE 802.11ac and co-developed the TAPs and WARP research platforms.

Edward received his Ph.D. degree from the University of California at Berkeley (US) in 1996. He was a visiting professor at EPFL (Switzerland). Currently, Edward is a Full Professor of Electrical and Computer Engineering at Rice University, Houston, Texas (US). He is an IEEE Fellow and an NSF CAREER award recipient.

For further information please contact: DLS@maki.tu-darmstadt.de

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de

Copyright Notice

Apologies for the inconvenience; but these days one is advised to better provide copyright notices even in lectures …

- This document has been distributed by the contributing authors as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that they have offered their works here electronically.
- It is understood that all persons copying this information will adhere to the terms and constraints invoked by each author's copyright. These works may not be reposted without the explicit permission of the copyright holder.