Peer-to-Peer Systems and Security
IN2194

Dipl.-Inform. Heiko Niedermayer
Christian Grothoff, PhD
Prof. Dr.-Ing Georg Carle
Course organization IN2194

- **Lecture**
  - Monday, 10:15-11.45, MI 00.13.009A weekly
  - Thursday, 14:15-15.45, MI 00.13.009A first weekly, then typically bi-weekly

- **Exercises**
  - Typically bi-weekly Thursday, 14:15-15.45, MI 00.13.009A

- **Students are requested to subscribe to lecture and exercises at**
  - [www.net.in.tum.de](http://www.net.in.tum.de) ⇒ lehre ⇒ vorlesungen ⇒ Informationen des Lehrstuhls
  - [http://www.net.in.tum.de/de/lehre/ss10/vorlesungen/vorlesung-peer-to-peer-systeme-und-sicherheit/](http://www.net.in.tum.de/de/lehre/ss10/vorlesungen/vorlesung-peer-to-peer-systeme-und-sicherheit/)

- **Email list, svn access**
  - for subscribers of course

- **Questions and Answers / Office hours**
  - Prof. Dr. Georg Carle, carle@net.in.tum.de
    - Upon appointment (typically Monday 16-17)
  - Heiko Niedermayer, niedermayer@net.in.tum.de
  - Christian Grothoff, Ph.D., grothoff@net.in.tum.de

- **Course Material**
  - Slides are available online. Slides may be updated during the course.
Grading

- Course is 5 ECTS
  - 3 SWS lectures
  - 1 SWS exercises
    - including practical assignment (programming project)

- Exercises
  - ~5 exercise sheets
  - Prepare for the oral examination
  - Successfully participating at exercises gives a bonus of 0.3 for overall grade

- Practical assignment
  - will be graded

- Our concept for grading
  - Final examinations will be oral and give an individual grade.
    - You must pass the oral exam for being successful in the course.
  - For overall grade, grade of practical assignment gives 20% of final grade
Questions

- Who studies what?
  - Diploma degree?
  - Master in Informatics?
  - Master in Information Systems [Wirtschaftsinformatik]?
  - Other Master courses?
  - Bachelor in Informatics?

- Which previous relevant courses?
Courses offered by I8

- **Lectures**
  - **SS:**
    - Introduction to Computer Networking and Distributed Systems (IN0010)
    - Discrete Event Simulation (IN2045)
  - **WS:**
    - Master Course Computer Networks (IN2097)
    - Network Security (IN2101)
- **Seminars**
  - Seminar – Network Architectures and Services: Network Hacking (IN0013)
  - Advanced Seminar - Innovative Internet Technologies and Mobile Communications (IN8901)
  - Advanced Seminar – Future Internet (IN8901)
  - Advanced Seminar – Sensor Networks (IN0014), with Prof. Baumgarten
- **Lab Courses**
  - Bachelor Practical Course - Internet Lab (IN0012)
  - Master Practical Course – Computer Networks (IN2106)
Motivation

The power of P2P
Peer-to-Peer Systems

Very popular due to file-sharing
Responsible for majority of the traffic of the Internet!

- Network of equals (peers)
  - Users can offer new services
- Users and their computers at the edges of the Internet share their resources (bandwidth, CPU, storage).
  - Inherent scalability with growing
- Self-organization of the system
  - No traffic management
- Autonomy from central entities like central servers
  - Robustness
Architecture of a Telecommunication Network (GSM)

- Involved in Authentication:
  - MS
  - BSS/MSC/VLR
  - HLR/AUC

- Network components:
  - MS
  - BTS
  - BSC
  - MSC
  - VLR
  - HLR
  - EIR
  - AUC
  - OMC
  - OSS
  - NSS
  - RSS

- Key signaling protocols:
  - ISDN, PSTN
  - PDN

- BSS (Base Station System)
- OMC (Operations and Maintenance Center)
- GMSC (Gateway Mobile Switching Center)
- IWF (Interworking Function)
- NSS (Network Switching Subsystem)
- OSS (Operations Support System)
- VLR (Visitor Location Register)
- HLR (Home Location Register)
- EIR (Equipment Identity Register)
- AUC (Authentication Center)
- OMC (Operations and Maintenance Center)
- ISDN (Integrated Services Digital Network)
- PSTN (Public Switched Telephone Network)
- PDN (Public Data Network)
### Some GSM Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUC</td>
<td>Authentication center</td>
</tr>
<tr>
<td>BSC</td>
<td>Base station controller</td>
</tr>
<tr>
<td>BSS</td>
<td>Base station system</td>
</tr>
<tr>
<td>BTS</td>
<td>Base transceiver station</td>
</tr>
<tr>
<td>IMSI</td>
<td>International mobile subscriber identity</td>
</tr>
<tr>
<td>HLR</td>
<td>Home location register</td>
</tr>
<tr>
<td>LAI</td>
<td>Location area identifier</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile station (e.g. a mobile phone)</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile switching center</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile subscriber international ISDN number</td>
</tr>
<tr>
<td>TMSI</td>
<td>Temporary mobile subscriber identity</td>
</tr>
<tr>
<td>VLR</td>
<td>Visitor location register</td>
</tr>
</tbody>
</table>

**Challenge:** Availability / Resilience
Related Research Activities at the Chair I8

- Goal:
  - Improve the resilience/security of network services
  - using the Peer-to-Peer networking paradigm
  - taking Voice over IP (VoIP) as an example
Cooperative SIP (CoSIP)

- User registration with CoSIP

  - User registration with CoSIP

  - User registration with CoSIP

- Session establishment with CoSIP

  - Session establishment with CoSIP

  - Session establishment with CoSIP

Cooperative SIP (CoSIP)

- User registration with CoSIP

  - User registration with CoSIP

  - User registration with CoSIP

- Session establishment with CoSIP

  - Session establishment with CoSIP

  - Session establishment with CoSIP

Cooperative SIP (CoSIP)

- User registration with CoSIP

  - User registration with CoSIP

  - User registration with CoSIP

- Session establishment with CoSIP

  - Session establishment with CoSIP

  - Session establishment with CoSIP
Application of CoSIP in the fixed network

- CoSIP adapter/ proxy in DSL routers
- CoSIP adapters organize themselves into a P2P network

Diagram:
- Small Office and Home Network (SOHO)
- DSL Router with a CoSIP adapter / CoSIP proxy
- Internet/VoIP Provider
- SIP Infrastructure

SOHO
EU FP7 Projekt ResumeNet

- “Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation”

- A EU Project of the FIRE Research Programme („Future Internet Research and Experimentation“)

- Consortium:

<table>
<thead>
<tr>
<th>ETH Zürich</th>
<th>Switzerland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lancaster University</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Technical University Munich</td>
<td>Germany</td>
</tr>
<tr>
<td>France Telecom</td>
<td>France</td>
</tr>
<tr>
<td>NEC Europe Ltd</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Universität Passau</td>
<td>Germany</td>
</tr>
<tr>
<td>Technical University Delft</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Uppsala Universitet</td>
<td>Sweden</td>
</tr>
<tr>
<td>Université de Liège</td>
<td>Belgium</td>
</tr>
</tbody>
</table>

- Strategy: D²R²DR
Robust Service Provisioning (Service Resilience)
Robust Service Provisioning (2)

- **Approach:**
  - Hybrid p2p overlay network
  - Peers with different roles, verifyable identity, virtualisation

- **Goal:**
  - Cooperation of end nodes and infrastructure for high reliability, service quality, scalability
Further selected research at I8– Network Architectures and Services
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EU ResumeNet</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>EU AuthoNe</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DFG LUPUS</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BMBF ScaleNet</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NSN SelfMan</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSN TC-NAC</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>France-Telecom SASCO</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BWFIT SpoVNet</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BWFIT AmbiSense</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AutHoNe - Autonomic Home Networking

- EUREKA-Celtic/BMBF-Project

- Partner in Germany
  - TU München
  - Fraunhofer FOKUS
  - Siemens Corporate Technology
  - Hirschmann Automation and Control

- EU/Celtic Partner
  - France Telecom, Frankreich
  - Sony-Ericsson, Schweden
  - Ginkgo Networks, Frankreich
  - Univ. Pierre et Marie Curie, Paris (UPMC-LIP6), Frankreich
  - Universität Lund, Schweden
Autonomic Home Networks

- Self-managed systems
- Visualization of the current state of the network
- Autonomic control
- "Plug and Play"

Adaptation to users and environment

Degree of Autonomicity

- Self-management
- Manual interaction

Intrusion detection

- Full control
- Trust determines access rights

Network: AutHoNe - Home Network

- Wired, Bluetooth
- Distributed sensor/actuator network

- Home gateway

Visitor

- Mobile devices
- Home monitoring probe

Monitoring probe

Autonomic home network

PC, Landlord

Landlord

Appliances

Visitor determines access rights
Basic concepts

- Knowledge Platform

- Autonomous Configuration and Management
Basic concepts

- User Control
  - User-friendly
  - Modes for normal users and experts

- Interaction with Environment
  - Sensors
  - Actuators
Home Networks with Cloud and P2P services

- AutHoNe provides Self-Management
  - Knowledge plane
  - Zero Configuration
- Cloud Computing
  - Computation and Storage in the network
  - Reliable resources
  - Pay and get more resources
  - Security Anchor → Provider and its accounting
- In combination with Peer-to-Peer
  - Use existing resources at edge
  - Scalability
  - Non-critical tasks and replication
- Bootstrapping and lookup of services
  - CloudCast to a near-by service cloud for lookup or processing
Detecting Command and Control Traffic

- Provider-guided attack detection in home networks
France-Telecom-Project SASCO: Overlay Security

- Project SASCO
  - Cooperation with France Télécom and Fraunhofer FOKUS

Situated Overlay

- Resource
- Access Control
- DMZ
- HSS
- Client
- Network Provider
- Geographic & Geodetic Information

Situated Overlay Nodes (SON)
SASCO: Situated Autonomic Service Control

Service Description

Service decomposition and Processing Chain calculation

Processing Chain

Negotiation of Service Parameters

Processing Chain instantiation and maintenance

Dynamic Access Control

Situated Overlay Network

Node 1

Node 2

Node 3

Server

P1

P2

P3

P4

P1

P2

P4

Client
BWFIT SpoVNet: Cross-Layer-Information for Overlays

- SpoVNet: Spontaneous Virtual Networks
- Flexible, adaptive and spontaneous service provisioning
- Approach: overlays
  - Let-1000-networks-bloom instead of One-size-fits-all
  - Tailored architecture for applications and networks
  - Cross-Layer-Information supports QoS decisions and optimisation
  - No dedicated infrastructure needed

Applications: Video Streaming, Gaming
SpoVNet - Spontaneous Virtual Networks

- Partners: KIT (Zitterbart), Uni Stuttgart (Kühn, Rothermel), Uni Mannheim (Effelsberg)
- Future Internet Approach
  - Locator/Identifier-Split
  - On demand overlay creation
  - Service overlays
  - UNISONO (@TUM)
  - Cross-layer Information Service
The lecture…
Course Overview

Chapter 1: Peer-to-Peer systems and overlay networks

Chapter 2: Security in distributed systems

Chapter 3: Anonymity and Privacy

Client/Server
Classic networking

Security
Peer-to-Peer Systems

- Network of equals
- No distinction between client and server
- Users and their computers at the edges of the Internet share their resources (bandwidth, CPU, storage).
- Self-organization of the system
- Autonomy from central entities like central servers
- Peers come and go → continuously changing environment

→ Very popular due to file-sharing and content distribution networks that today are responsible for majority of the traffic of the Internet
... but …

- Highly decentralized systems are not very secure.
- What about peers that do not cooperate?
- What about attacks or misuse?

... still….

- Peer-to-Peer systems are useful for censor-resistance, DoS resilience, etc.

Security is an important issue especially for serious applications. Decentralized systems have their drawbacks, but also a high potential for improvements!
Anonymity & Privacy

- In our daily life we are often an anonymous entity among a mass of other entities.

- Pseudonymity: An entity hides behind a pseudonym, so that anyone (but an authority) only knows the pseudonym, but not the true identity. The pseudonym can be tracked.

- Anonymity: Hide the identity, the usage/traffic patterns, and relationships from other entities or observers. No tracking.

→ Traffic Analysis can reveal information that is leaked even if encryption is used. Technologies like Onion Routing can make these attacks harder.
Where are we?

... on the network stack...

... on application layer with some exceptions.
Where are we? II

Who is contributing / doing the work?