Peer-to-Peer Systems and Security
IN2194

Dr. 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

- **Website**
  - www.net.in.tum.de ➔ lehre ➔ vorlesungen ➔ Informationen des Lehrstuhls
  - http://www.net.in.tum.de/de/lehre/ss11/vorlesungen/vorlesung-peer-to-peer-systeme-und-sicherheit/

- **SVN access**
  - Subcribe on website

- **Questions and Answers / Office hours**
  - Prof. Dr. Georg Carle, carle@net.in.tum.de
    - Upon appointment (typically Monday 16-17)
  - Dr. 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)

- Grading
  - Final examinations will be oral and give an individual grade.
  - You must pass the oral exam for being successful in the course.
  - Oral Exam 50 %
  - Practical Assignment 50 %
  - 0.3 bonus for passing the exercises

- Exercises (~ 5 exercise sheets)
  - Success = 70 % of the tasks submitted, present at >= 3 exercises and 1x presentation of a solution
  - Goal: Prepares for the oral examination

- Practical assignment
  - Introduced in the 2nd half of the first lectures
  - Goal: Practically apply the concepts and learn to use them.
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
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

- Session establishment with CoSIP

User registration with CoSIP:

1. User Alice registers with CoSIP using the REGISTER method.

2. Alice's contact URI is stored in the DHT.

Session establishment with CoSIP:

1. Alice initiates a session by sending a SIP INVITE message to Bob.

2. The DHT is queried to locate Bob's contact URI.

3. Alice sends a CoSIP INVITE message to Bob containing Bob's contact URI.
Application of CoSIP in the fixed network

- CoSIP adapter/ proxy in DSL routers
- CoSIP adapters organize themselves into a P2P network
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: $D^2R^2DR$

Diagram:
- Policies
  - Diagnose – Refine feedback loop (long-term)
  - Recovery feedback loop (real-time)
- Network management
- Service management
- Monitoring
- Detect and Diagnose
- Remediate
- Context information
- Refine
Robust Service Provisioning (Service Resilience)

- Alice sends a SIP INVITE request to Bob.
- Bob receives the SIP INVITE and responds with a Contact URI.
- Alice sends another CoSIP INVITE to Bob.

Diagram:
- Alice and Bob are connected via a P2P network.
- The interaction is illustrated with arrows indicating the flow of messages.
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

---

AAA/IdM servers
SIP Proxies
PSTN gateways
eNodeBs
Home (e)NodeBs/WiFi routers
Mobile devices
Further selected research at I8– Network Architectures and Services
## Projektschwerpunkte

<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

Adaptation to users and environment

Degree of Autonomicity

Self-management

Manual interaction

AutHoNe - Home Network
• Self management
• Visualization of Network State
• Autonomic Control
• "Plug and Play"

Visitor

Trust determines Access Rights

Monitoring Probe

Distributed Sensor/Actuator Network

Home Gateway

Full Control

Mobile Devices

WLAN, Bluetooth

PC

Appliances

Landlord

IN2194: Peer-to-Peer Systems and Security, SS 2011
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

![Diagram showing the flow of security information from Home Network to Provider through Alert!!! mechanisms connected to Control server, Bot-Master, Malware, Internet, and Local Network.]
Project SASCO

- Cooperation with France Télécom and Fraunhofer FOKUS

Situated Overlay

- Situated Overlay Nodes (SON)
- Geographic & Geodetic Information

DMZ

- Resource
- Access Control

Network Provider

- HSS
- Client

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

Negotiation of Service Parameters

Dynamic Access Control

Situated Overlay Network

Service Description

Service decomposition and Processing Chain calculation

Processing Chain

Processing Chain instantiation and maintenance
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…
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!
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...

<table>
<thead>
<tr>
<th>Layer 7</th>
<th>Layer 4</th>
<th>Layer 3</th>
<th>Layer 2</th>
<th>Layer 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer (e.g. HTTP)</td>
<td>Transport Layer (e.g. TCP, UDP)</td>
<td>Network Layer (e.g. IP)</td>
<td>Data Link Layer</td>
<td>Physical Layer</td>
</tr>
</tbody>
</table>

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

Who is contributing / doing the work?