Organizational Overview

Dr.-Ing. Kalman Graffi
Faculty for Electrical Engineering, Computer Science at the University of Paderborn
Tools to be used

Web

EasyChair
- For seminar paper & reviews management
- [http://www.easychair.org/conferences/?conf=p2pseminar2012](http://www.easychair.org/conferences/?conf=p2pseminar2012)

Simulator to use: PeerfactSim.KOM – UPB-Fork
- [www.peerfact.org](http://www.peerfact.org)
- Visit website for documentation

Doodle for topic selection
- [https://www.doodle.com/crtzpba2hgurarxx](https://www.doodle.com/crtzpba2hgurarxx)
Seminar Schedule

11. April 2012
- Organizational details
- Presentation of the topics
- Time for questions

11.-17. April 2012
- Doodle-based choosing of seminar topics
  - https://www.doodle.com/crtzpba2hgurarxx

18. April 2012
- Assignment to the topics
- Simulator open hours: http://www.doodle.com/xbyhzuunqthew2mzz
Seminar Schedule

May / June 2012

- Time to work on the topic
- Content-related questions:
  - Per email (graffi@mail.upb.de)
  - In person: schedule meeting first per email
- Simulator-related questions
  - Weekly meetings
  - Date to be found via Doodle → 25. April 2011
  - https://www.doodle.com/xbyhzuunqwh2mzz

10. June 2012

- Register your paper in EasyChair

17. June 2012

- Bid for the papers that you would like to review
Seminar Schedule

24. June 2012
- Submit seminar paper
  - Deadline: 23:59
- Receive 3 seminar papers to review

1. July 2012
- Submit 3 reviews to the seminar papers you got
  - Deadline: 23:59
- Submit presentation slides

8. July 2012
- Include the feedback
  - of your reviews
  - to your presentation slides
- Submit your final seminar paper and presentation slides
  - Deadline: 23:59

- Block seminar → presentations from 11:00 – 20:00
- Room: ...
Presentation of results

Deliveries:
- Seminar paper
  - 8+ pages
  - IEEE tran style (see template on website)
- Presentation
  - 25 minutes talk + 5 minutes discussion
- PPTX template

Grading components
- Paper quality
- Scientific content
  - Also with respect to desired module
- Writing style
- Review quality
- Effort to give valuable feedback
- Presentation quality

The Title of your Seminar Paper

Your Name
Student number: 12345678
Email: YourEmail@email.com
University of Paderborn, UPB - WS 2012/2013 - Peer-to-Peer Systems Seminar

Abstract—The abstract of your seminar paper

1. INTRODUCTION

Motivation of your seminar paper, see Figure 1. In Section II we continue.

II. NEXT SECTION

Lorem ipsum dolor sit amet, consectetur adipiscing elit [1], sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusant elit, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusant elit, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Table 1 is placed at the end of this section. The abstract is completed in Section II.

TABLE I

<table>
<thead>
<tr>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>C</td>
</tr>
</tbody>
</table>

REFERENCES
Grading components → every submission counts

- Seminar paper:
  - First version
  - Final version
  - Criteria
    - Scientific content
      » Also with respect to desired module
    - Writing style

- Review quality
  - Effort to give valuable feedback

- Presentation quality
  - Time
  - Content
Seminar Topics and Assignment
Seminar Topics

1: Networking Algorithms (MuA)
   1.1. Coordinated consensus in dynamic networks
   1.2. Wuala: security analysis and performance bounds: Cryptree and Havelaar
   1.3. Attacks on replication-based storage systems

2: Security in Practical Networks (ESS)
   2.1 Attacks on LifeSocial: a p2p-based online social network
   2.2 Access-control lists for distributed data structures in malicious networks
   2.3 Attacks on quality monitoring solutions in p2p systems

3. Evaluating the Impact of Attacks in P2P Networks (ESS, 2 in a team):
   3.1 Sybil and eclipse attacks in Chord (attacking single nodes or data)
   3.2 Sybil and eclipse attacks in Pastry (attacking single nodes or data)
   3.3 Routing attacks in Pastry (False Routing)
   3.4 Routing table poisioning in Pastry
   3.5 Replication attacks on the replication layer (and Pastry)
## Topic Assignment

<table>
<thead>
<tr>
<th>Topic</th>
<th>Title</th>
<th>Matrikelnr</th>
<th>Name</th>
<th>Vorname</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>1.1. Coordinated consensus in dynamic networks</td>
<td>6638258</td>
<td>Peng</td>
<td>Weifeng</td>
</tr>
<tr>
<td>1.2</td>
<td>1.2. Wuala: security analysis and performance bounds: Cryptree and Havelaar</td>
<td>6670785</td>
<td>Wang</td>
<td>Yuankui</td>
</tr>
<tr>
<td>1.3</td>
<td>1.3. Attacks on replication-based storage systems</td>
<td>6640590</td>
<td>Raza</td>
<td>Dauran</td>
</tr>
<tr>
<td>2.1</td>
<td>2.1 Attacks on LifeSocial: a p2p-based online social network</td>
<td>6241356</td>
<td>Zhu</td>
<td>Xiuqi</td>
</tr>
<tr>
<td>2.2</td>
<td>2.2 Access-control lists for distributed data structures in malicious networks</td>
<td>6643395</td>
<td>Neelkanth</td>
<td>Aditya</td>
</tr>
<tr>
<td>2.3</td>
<td>2.3 Attacks on quality monitoring solutions in p2p systems</td>
<td>6197774</td>
<td>Zhao</td>
<td>Hongying</td>
</tr>
<tr>
<td>3.1</td>
<td>3.1 Sybil and eclipse attacks in Chord</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>3.2 Sybil and eclipse attacks in Pastry</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>3.3 Routing attacks in Pastry</td>
<td>6465811</td>
<td>Eichert</td>
<td>Felix Alexander</td>
</tr>
<tr>
<td>3.4</td>
<td>3.4 Routing table poisoning in Pastry</td>
<td>6511219</td>
<td>Sander</td>
<td>Jan Marcel</td>
</tr>
<tr>
<td>3.5</td>
<td>3.5 Replication attacks on the replication layer (and Pastry)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Open Topics

<table>
<thead>
<tr>
<th>Student ID</th>
<th>Name</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>6465811</td>
<td>Eichert Felix</td>
<td>3.3 Routing attacks in Pastry (False Routing)</td>
</tr>
<tr>
<td>6484380</td>
<td>El Gharbawy</td>
<td>Mohamed Said Mohamed</td>
</tr>
<tr>
<td>6664306</td>
<td>Hammons Mark</td>
<td></td>
</tr>
<tr>
<td>6492981</td>
<td>Janiuk Jens</td>
<td>3.4 Routing table poisoning in Pastry</td>
</tr>
<tr>
<td>6437893</td>
<td>Kohlos Andreas</td>
<td></td>
</tr>
<tr>
<td>6477031</td>
<td>Monhof Markus</td>
<td>3.3 Routing attacks in Pastry (False Routing)</td>
</tr>
<tr>
<td>6643395</td>
<td>Neelkanth Aditya</td>
<td>2.2 Access-control lists for distributed data structures in malicious networks</td>
</tr>
<tr>
<td>6638258</td>
<td>Peng Weifeng</td>
<td>1.1. Coordinated consensus in dynamic networks</td>
</tr>
<tr>
<td>6640590</td>
<td>Raza Dauran</td>
<td>1.3. Attacks on replication-based storage systems</td>
</tr>
<tr>
<td>6511219</td>
<td>Sander Jan Marcel</td>
<td>3.4 Routing table poisoning in Pastry</td>
</tr>
<tr>
<td>6670785</td>
<td>Wang Yuankui</td>
<td>1.2. Wuala: security analysis and performance bounds</td>
</tr>
<tr>
<td>6197774</td>
<td>Zhao Hongying</td>
<td>2.3 Attacks on quality monitoring solutions in p2p systems</td>
</tr>
<tr>
<td>6241356</td>
<td>Zhu Xiuqi</td>
<td>2.1 Attacks on LifeSocial: a p2p-based online social network</td>
</tr>
</tbody>
</table>
1: Networking Algorithms (MuA)

1.1. Coordinated consensus in dynamic networks

- Fabian Kuhn, Yoram Moses and Rotem Oshman

Consensus:

- Agreement of nodes
- Hard to do under dynamics

Theoretical paper that you should present and explain
1.2. Wuala: security analysis and performance bounds: Cryptree and Havelaar

- **Cryptree**: A Folder Tree Structure for Cryptographic File Systems
  - Dominik Grolimund, Luzius Meisser, Stefan Schmid, Roger Wattenhofer
- **Havelaar**: A Robust and Efficient Reputation System for Active Peer-to-Peer Systems
  - Dominik Grolimund, Luzius Meisser, Stefan Schmid, Roger Wattenhofer

**Wuala**

- Commercial P2P / cloud storage
- Secure and performant
- Architecture partially published

Give overview on technology and model the file availability and security
1: Networking Algorithms (MuA)

1.3. Attacks on replication-based storage systems

- Overview on approaches for replication,
- Select most prominent top 2-3,
- Define models for attackers

- Model the replication system:
  - What is the minimum ratio of replication needed under the various attacks and churn to reach a desired availability
  - What is the influence of file sizes, node online behaviour, attack strategies
  - How is the storage and retrieval costs and performance

Papers:

- R. Hasan, “A survey of peer-to-peer storage techniques for distributed file systems”, in ITCC 2005
2: Security in Practical Networks (ESS)

2.1 Attacks on LifeSocial: a p2p-based online social network

Fully p2p-based social network
- Developed since 2007
- Aiming at applicable results in p2p research

Goal
- Facebook-like user experience
- Fully P2P → (See also PG: P2P Framework for Social Networks)

Question covered in seminar:
- Investigation of attacks on the architecture of LifeSocial
- Analyze and discuss weaknesses of 
  - FreePastry / PAST / security components …

Papers:
- K. Graffi et al. „LifeSocial.KOM: A Secure and P2P-based Solution for Online Social Networks“. In IEEE CCNC 2011
- K. Graffi et al., „Practical Security for P2P-based Social Networks“. IEEE LCN 2009
- K. Graffi et al. „A Distributed Platform for Multimedia Communities“. IEEE ISM 2008
2: Security in Practical Networks (ESS)

2.2 Access-control lists for distributed data structures in malicious networks

- Case: distributed data storage in structured p2p overlay
- Problem: malicious nodes want to corrupt the data
- Give overview on research solutions and applicability in Pastry
  - Systematic classification of solutions
  - Apply evaluation scheme: How to judge whether a solution is good

Papers:
- R. Hasan, “A survey of peer-to-peer storage techniques for distributed file systems”, in ITCC 2005
2.3 Attacks on quality monitoring solutions in p2p systems

Monitoring: gathering statistics in the p2p network
- Approach: Either gossip-based or tree-based
- Problem: Malicious nodes might falsen the statistics

Goal of the paper:
- Systematic overview and discussion of
  - Attack approaches and security solutions

Papers:
- D. Kempe et al., „Gossip-based computation of aggregate information”, in IEEE Foundations of Computer Science, 2003
3. Evaluating the Impact of Attacks in P2P Networks (ESS)

3.1 Sybil and eclipse attacks in Chord
   ▪ (attacking single nodes or data)

3.2 Sybil and eclipse attacks in Pastry
   ▪ (attacking single nodes or data)

3.3 Routing attacks in Pastry (False Routing)

3.4 Routing table poisoning in Pastry

3.5 Replication attacks on the replication layer (and Pastry)
3. Evaluating the Impact of Attacks in P2P Networks (ESS)

Papers:

Sybil attacks:
- G. Danezis et al. “Sybil-resistant DHT Routing,” in ESORICS 2005

Routing attacks in Pastry:
- C. Gottron et al., “A Testbed-based Analysis of the Incorrect Lookup Routing Attack on the Pastry DHT”, EUROVIEW

Replication attacks:
Language and Presentation

Language:
- Spell check! Use programs for it!
- Spell check by human

Figures
- Use only scalable vector graphics
  - Infinitively zoomable
  - Exception: screenshots
- Be careful with colors (do not use them):
  - Papers will be printed black/white
Next Steps

Web
- https://www.cs.uni-paderborn.de/index.php?id=17072

Doodle for simulator open hours
- http://www.doodle.com/xbyhzuunqwh2mzz

26. April 2012
- Doodle-based choosing of simulator open hours (Topics 3.*)
- Lecture on PeerfactSim.KOM (Topics 3.*)

EasyChair
- For seminar paper & reviews management
- http://www.easychair.org/conferences/?conf=p2pseminar2012

Simulator to use: PeerfactSim.KOM – UPB-Fork
- www.peerfact.org
- Visit website for documentation