Concepts of Trust Establishment
WS 2023/24
Seminar

Maximilian von Tschirschnitz

Lehrstuhl für Sicherheit in der Informatik / I20
Prof. Dr. Claudia Eckert
Technische Universität München

July 4, 2023
What is this seminar about?

Grasping the concepts of Trust and how we can establish it (autonomously).

- What does the relation of Trust actually mean?
- What established/novel concepts of Trust Establishment are available?
- What Axioms can we choose from to rely upon?
Process

- **Phase I**: Select a topic
- **Phase II**: Find literature
- **Phase III**: Do your reading / experiments / programming
- **Phase IV**: Writing phase I
- **Phase V**: Peer review
- **Phase VI**: Writing phase II
- **Phase VII**: Final talks

Exact schedule will be published once list of participants is known.
Phase I

1. I will provide you with a list of starting points for topics that are of interest for this seminar

2. You will **choose / propose** your topic and thereby either:
   ▶ Model, analyse or compare some existing definitions of, and approaches to Trust.
   ▶ Conduct a critical analysis of an existing Trust establishment method
   ▶ Elaborate on novel (cryptographic) approaches (e.g. Homomorphic Time Lock Puzzles)
   ▶ Categorize existing Trust establishment methods
   ▶ Elaborate on concepts of tracking/trusting origin

3. In all cases, you will put your work into context of existing literature
   ▶ e.g at Usenix Security Symposium, S&P, ACM CCS, NDSS
Our Topics of Interest

- Proximity as Trust Factor
- Trustmanagement in Groups/Teams
- Survey on Trust establishment in Ad hoc networks
- Game Theory applied to Ad Hoc networks
- Integrity Codes / Tamper Evident Pairing
- Differentiation of available ‘Web of Trust’/PKI Concepts
- Comparison of formal verification approaches
- Homomorphic Time Lock Puzzles
- Provenance and Dependency Analysis in relation to Authenticity
- Password Authenticated Key agreement and Zero Knowledge Proofs

Or: Provide me with your own topic proposal and I will consider it
Registration

- Registration using the **matching system**
- Letter of motivation gets preference
- Email **one paragraph** why you want to do this seminar
- Your interests/skillset for that course
- Send **with subject** [CTE] to tschirschnitz@sec.in.tum.de
Time and Place

When?  
- I pick the slot
- ① for Bi-Weekly Meetings during the Semester
- ② with the least collisions
- ③ Physical attendance mandatory!

Talks at the end of the semester
Time and Place

When? I pick the slot
① for Bi-Weekly Meetings during the Semester
② with the least collisions
③ Physical attendance mandatory!

Talks at the end of the semester
<table>
<thead>
<tr>
<th>Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Paper (Content, Style, Language, Scope, ...)</td>
<td>40 %</td>
</tr>
<tr>
<td>Practical application (depends on topic)</td>
<td>10 %</td>
</tr>
<tr>
<td>Review</td>
<td>10 %</td>
</tr>
<tr>
<td>Presentation (Content, Style, Timeliness, ...)</td>
<td>30 %</td>
</tr>
<tr>
<td>Discussion</td>
<td>10 %</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100 %</strong></td>
</tr>
</tbody>
</table>
Questions?

Contact me at
tschirschnitz@sec.in.tum.de