Common Flaws in Protocolsecurity — WS 2022/23
Seminar

Maximilian von Tschirschnitz & Ludwig Peuckert

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

July 19, 2022
What is this seminar about?

- **Design flaws** in communication protocols
- **Mitigations**, Fuzzing, Verification, Code Generation
- **Lessons learned**: Effect on later protocol generations
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.
1. We will provide you with a list of our topics of interest
2. You will choose / propose your own topic and either:
   ▶ Work out the crucial design flaw
   ▶ Elaborate on mitigations and impact on protocol security
   ▶ Reproduce the results of an existing conference paper
   ▶ Create your own Systematization of Knowledge (SoK) paper
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

▶ Specific Attacks (e.g. Downgrade, Replay)
▶ Implementation Specific Bugs (e.g., Heartbleed, Ping of Death)
▶ Trust Establishment Design Principles (PKI, Web of Trust, TLS)
▶ Formal Verification for Protocols
▶ Automatic Code Generation/Validation from Specification
▶ Or: Provide us with your own topic proposal
Registration

- Registration using the **matching system**
- **No** letter of motivation
- approx. 8 slots
Time and Place

**When?**
- Tuesdays 14:00 - 16:00 roughly Bi-Weekly
  - ① Some meetings will be canceled or replaced
  - ② First meeting in the first lecture week
  - ③ First task before first meeting

Talks at the **end** of the semester

**Where?**
Time and Place

When? Tuesdays 14:00 - 16:00 roughly Bi-Weekly
1. Some meetings will be canceled or replaced
2. First meeting in the first lecture week
3. First task before first meeting

Talks at the end of the semester

Where? Seminartagungsstätte Frauenchiemsee

Disclaimer: Only if participants show interest!
Fallback: On-campus conference
Grading

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>40%</td>
<td>Final Paper (Content, Style, Language, Scope, ...)</td>
</tr>
<tr>
<td>10%</td>
<td>Practical application (depends on topic)</td>
</tr>
<tr>
<td>10%</td>
<td>Review</td>
</tr>
<tr>
<td>30%</td>
<td>Presentation (Content, Style, Timeliness, ...)</td>
</tr>
<tr>
<td>10%</td>
<td>Discussion</td>
</tr>
</tbody>
</table>

\[ \Sigma \ 100\% \quad \text{Total} \]
Questions?

Contact us at
maximilian.tschirschnitz@sec.in.tum.de,
peuckert@sec.in.tum.de

https://www.sec.in.tum.de/i20/teaching/ws2022/common-flaws-in-protocol-security