




Encryption

Exercise 5.1 (/)

1. Split into working groups of 3 or 4 students
2. Each group is assigned one of the topics (by consensus or randomization) described on the following slides
3. Until the next lecture, every group prepares a digital presentation of 15-20min on their topic
4. At least *2 days before* the next lecture a PDF export of their presentation is sent to bjoern.kimminich@nordakademie.de
5. During the next lecture all groups present their topic to their classmates

Presentation Format

- 15-20min presentation
 - *every* group member *has to* present for at least 5min
- 5-10min Q&A

 *The presentation can be written and held in  or  based on each group's own preference. Just do not mix English and German slides. English slides but presentation held in German is fine.*

Presentation Topics

1. [WEP](#) ⚡ [FMS & Chopchop](#)
2. [WPA2](#) ⚡ [KRACK](#)
3. [PGP](#) ⚡ [EFAIL](#)
4. [SSL/TLS](#) ⚡ [POODLE](#) & [DROWN](#)
5. [BitLocker](#) ⚡ [TCG Opal](#)

💡 *The links provided are some documentation/specification (if publicly available) as well as vulnerability research papers. Each group is supposed to gather additional references as needed.*

Presentation Structure

1. Introduction of the protocol/system
2. Explanation of the attack(s)
3. Mitigation of the attack(s)
4. Recommendations or related information

 *Please provide a list of sources referred to in the presentation as the final slide.*

Timeline

- Thu, 22.11.2018 (*today*)
 - Group building, topic assignment & initial research
- Tue, 04.12.2018 (*+12d*)
 - All PDF-exported presentations delivered to bjoern.kimminich@nordakademie.de
- **Thu, 06.12.2018** (*+2d*)
 - **All groups present their topics** between 09:15 and 13:00