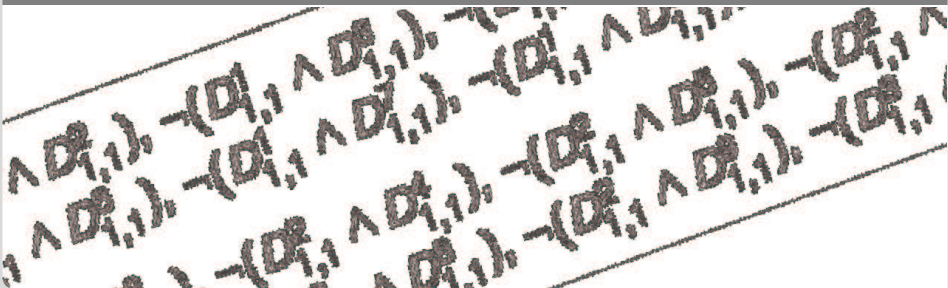


Desaster in der Software-Sicherheit

Proseminar in WiSe15/16

Bernhard Beckert

Institute for Theoretical Informatics, KIT



HoC-Mikromodul: Präsentationstraining für Studierende der Informatik (Bachelor)

Ziele

- Vermitteln von Präsentations-Grundlagen
- Verbesserung der Präsentationskompetenz,
- insbesondere im Hinblick auf den Vortrag im Proseminar

Inhalte

- Vorbereiten, Durchführen und Nachbereiten von Präsentationen
- Präsentationen im Spannungsfeld Person, Inhalt, Kontext
- Zieldimensionen von Präsentationen
- Strukturieren von Präsentationen
- Nonverbale und paraverbale Aspekte beim Präsentieren

HoC-Mikromodul: Präsentationstraining für Studierende der Informatik (Bachelor)

Organisatorisches

- Insgesamt 2 Termine:
Di, 01.12. 2015 8:45 – 12:45 Uhr und
Mo, 07.12.2015 8:45 – 12:45 Uhr
- 1 ECTS Überfachliche Qualifikationen
- verbindliche Anmeldung (9.11.2015 12:00 bis 17.11. 2015 24:00 Uhr)
unter: <https://portal.wiwi.kit.edu/Courses/Event/Details/62def563-a9b3-c847-885c-7475dcf3e332>

Leistungen der Studierenden

- Aktive Teilnahme an den zwei Terminen
- Erstellen einer 5-minütigen Präsentation zum im Proseminar gewählten Thema anhand von Leitfragen
- Präsentieren im Training inkl. Feedback und Video-Feedback

Aufgabenpunkte

- Verstehen des Stoffes
- Auswahl der Themen, die präsentiert werden sollen
- Planung des Vortrags
- Erstellen der Folien
- Vortrag (30 Minuten)
- Schriftliche Ausarbeitung (5-10 Seiten)

Ablauf

- Entscheidung Teilnahme / Themenzuordnung bis Ende der Woche, 23.10. (first come first serve)
- E-Mail an `meinhardt@kit.edu` mit Präferenzliste für die Themen und Angabe ob Teilnahme am HoC-Modul
- Blockseminar
- 2 Tage gegen Ende des Semesters
- Zwischenpräsentation (je 5 Minuten) in KW 50 (2. Dezemberwoche)
- vor der Präsentation:
Anmeldung zum **Proseminar Containermodul 201**

- 1 Buffer-Overflow Angriffe (AW)
- 2 Patriot Rocket Disaster (MH)
- 3 Android Malware (VK)
- 4 Knightmare on Wall Street (DG)
- 5 Taint Analysis für Adroid Apps (SG)
- 6 Secure Multi-Execution (SG)
- 7 Storing Passwords (AW)
- 8 Replacing Testing with Formal Verification (MU)
- 9 Treiberverifikation mit SLAM (SaG)
- 10 ASLR, its Failures, and Related Measures (VK)
- 11 Cryptocurrencies and Attacks on Them (VK)
- 12 How much testing is enough? (TB)
- 13 Voting Paradoxes (MK)
- 14 Sichere elektronische Wahlen (MK)