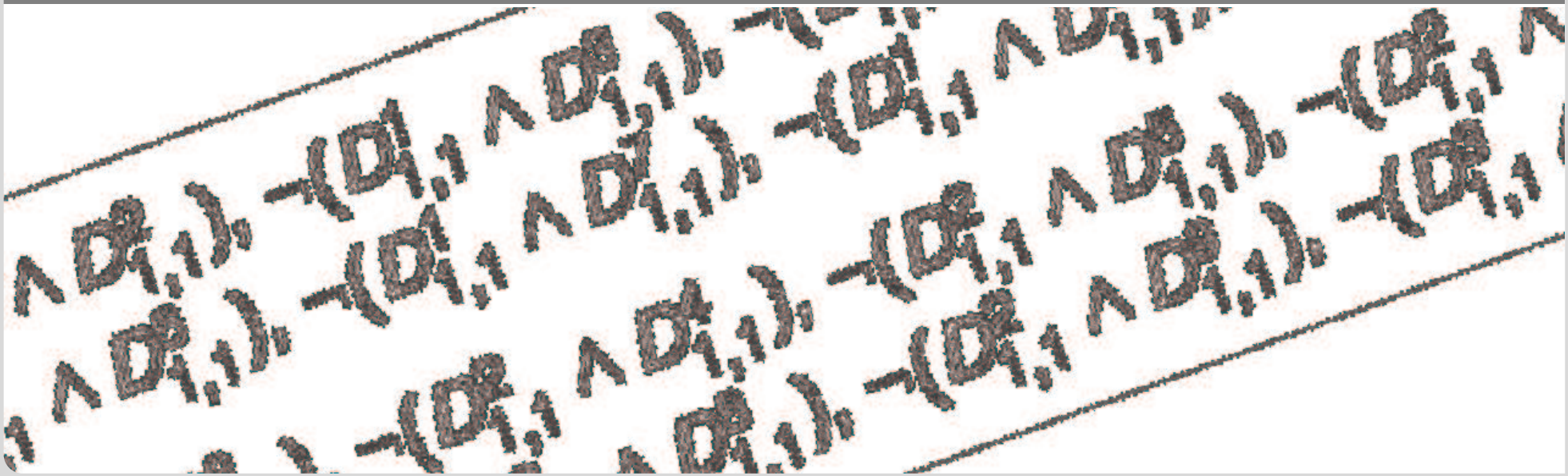
Karlsruher Institut für Technologie

Desaster in der Software-Sicherheit: Können formale Methoden helfen? Proseminar in SoSe 2016

Bernhard Beckert

Institute for Theoretical Informatics, KIT



Organisatorisches

Aufgabenpunkte

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

Organisatorisches

Ablauf

- Entscheidung Teilnahme / Themenzuordnung bis Ende der Woche, 22.04.16, 14 Uhr (Reihenfolge in Anmeldungsreihenfolge)
- E-Mail an `meinhart@kit.edu` mit Präferenzliste für die Themen
- bis 08.06.16:
  Prüfungsanmeldung zum **Proseminar** (siehe Handout)

- Zwischenpräsentation:
  je 5 Minuten, nach ca. 6 Wochen
  (Folien 1 Woche davor)
- Hauptpräsentation:
  Blockseminar, 2 Tage am Semesterende
  (Folien 1 Woche vor 1.Termin)

Themen

1. Verifikation von probabilistischen Sicherheitsprotokollen (AW)
2. Verifikation von medizinischen Richtlinien mit Model-Checking (AW)
3. Informationsflussanalyse mit Programmabhängigkeitsgraphen am Beispiel JOANA (SG)
4. Formale Verifikation von Kryptographischen Protokollen am Beispiel ProVerif (SG)
5. Ironclad Apps: End-to-End Security via Automated Full-System Verification (TB)
6. Are We There Yet? Determining the Adequacy of Formalized Requirements and Test Suites (TB)
7. Neue Trends in der Autoaktiven Verifikation (SaG)
8. Exploit-Generation für Informationsflusseigenschaften (MH)

Themen (cont'd)

9. Automatisches Finden von Exploits mittels Fuzzing und Symbolic Execution (oder: Wie Man $ 750 000 Gewinnt) (MK)
10. Judgement Aggregation (BB)
11. Fehler in Hardware vermeiden durch Äquivalenzbeweise (MU)
12. Angriffe auf die IT-Sicherheit bei elektronischen Wahlen (t.b.a.)