

Hauptseminar: Nachweis von Sicherheitseigenschaften für JavaCard durch approximative Programmauswertung

Prof. Tobias Nipkow, Martin Strecker

WS 2001 / 2002

Überblick

- Einführung: Wovon handelt das Seminar?
- Themenüberblick
- Organisatorisches
- Themenvergabe

Themenüberblick (1)

1. *JavaCard: Hardware-nahe Aspekte*
 - Chen: JavaCard Technology for SmartCards. Addison-Wesley 2000. Kap. 2-5
 - Lanet et al.: Checking Secure Interactions of Smart Card Applets
2. *JavaCard: Applet firewall und Shareable Interfaces:*
 - Chen, Kap. 9
3. *Temporallogik*
 - *Grundlagen CTL*: Huth/Ryan: Logic in Computer Science. Cambridge University Press, 2000
 - Jensen; Le Metayer; Thorn: Verification of control flow based security properties
 - *Modelchecker SMV* (optional): SMV-Tutorial
4. *SDL*
 - – *Überblick über SDL* Belina; Hogrefe; Sarma: SDL with applications, Prentice Hall/Hanser 1991
 - *Modellierung der Gemplus-Fallstudie mit SDL*

Themenüberblick (2)

5. μ -Kalkül

- *Grundlagen μ -Kalkül*: Modellierung von Sicherheitseigenschaften im μ -Kalkül
- Barthe; Gurov; Huisman: Compositional Specification and Verification of Control Flow Based Security Properties of Multi-Application Programs
- *Modelchecker Mucke* (optional): Diss. A. Biere/ Mucke-Tutorial

6. Abstrakte Interpretation und Datenfluß-Analyse

- *Grundlagen*:
 - Muchnik: Advanced Compiler Design. Morgan Kaufmann 1997
oder Wilhelm; Maurer: Übersetzerbau. Springer 1997
- Bourdoncle: Assertion-Based Debugging of Imperative Programs by Abstract Interpretation

7. Java Bytecode-Verifikation

- – Lindholm; Yellin: The JVM Specification, 2nd ed., Addison-Wesley 1999. Kap. 4.9
- Klein; Nipkow: Verified Bytecode Verifieres. TCS, to appear

8. Verifikation mit Unterstützung von Theorembeweisern

- Detlefs et al.: Extended Static Checking

Organisatorisches

Veranstaltungsform:

- Wöchentlich 1 oder 2 Vorträge
- Regelmäßige Teilnahme wird erwartet
- Genaue Termine: Siehe Web-Seite

Zeitlicher Rahmen:

- Themenvergabe: Sofort...
- Literatur: Bei Martin Strecker abholen (innerhalb der nächsten Tage)
- Schriftl. Bericht (Entwurf): **3 Wochen vor Vortrag**
- Schriftl. Bericht (endgültige Form): **2 Wochen vor Vortrag**
- Vortragsfolien (Entwurf): **2 Wochen vor Vortrag**
- Vortragsfolien (endgültige Form): **1 Woche vor Vortrag**

Bei Problemen: Frühe Rücksprache mit Betreuer!

Schriftlicher Bericht

- Länge: 15 (± 3) Seiten pro Vortrag
- Bei gemeinsamen Vorträgen *dürfen* gemeinsame Ausarbeitungen abgegeben werden
- Sprache: Deutsch / Englisch
- Textverarbeitung:
 - Bevorzugt \LaTeX
 - Formatvorlagen: Siehe Web-Seite
 - Endgültiges Dokument als Postscript oder PDF

Vortrag

- Länge: 45 Minuten + 15 Min. Diskussion pro Vortragendem
- Bei gemeinsamen Vorträgen: Gleiche Verteilung der Vortragszeit
- Sprache: Deutsch / Englisch
- Präsentation:
 - Folien oder Beamer
 - Formatvorlagen für Folien mit \LaTeX : Siehe Web-Seite
 - Für Vortrag kann Linux-Laptop gestellt werden
 - Vortrag mit MS-Produkten: Eigene Verantwortung

Bericht und Vortrag - Schwerpunkte

- Beschreibung des Ansatzes auf informeller Ebene
- Darstellung einiger “interessanter” techn. Einzelheiten
- Abgrenzung zu anderen Methoden / Formalismen
z.B. CTL / μ -Kalkül
- Einschätzung der Methode:
 - Verständlich? Gut anwendbar?
 - Hält sie ihr Versprechen?
 - Erweiterbarkeit?