Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Non-functional properties in Operating Systems and Middleware

Seminar

Frank Feinbube, Christian Neuhaus, Lena Feinbube

Prof. Dr. Andreas Polze

Organization

- Schedule: Thursday, 13.30-15.00
- Attendance required
- Grading based on:
  - Presentation
    - Discuss agenda and draft before giving the talk
  - Written report
    - 8-12 pages LNCS or 4-6 pages IEEE
    - Discuss table of contents and draft before handing in the report

Focus: Security

- (Sicherheitseigenschaften) und Zertifizierungen (Common Criteria, FIPS 140-2)
- Gehärtete Unixoide Betriebssysteme (z.B. Trusted Solaris, Solaris Trusted Functionality, Trusted BSD, Hardened BSD, Hardened Linux)
- Flux Advanced Security Kernel (FLASK) (OS-Sicherheitsarchitektur)
- Sicherheit in Windows (Security Manager)
- Provably Secure Operating Systems und Object-Capability Systems
  - (e.g seL4, KeyKOS, EROS)
- Neue Anwendungen der Blockchain-Technologie
  - Decentralized Notary, Smart Contracts, etc.
- Middleware Security Models (e.g CORBA, .NET, J2EE)
- Maftia Middleware (Malicious-and Accidental-Fault Tolerance for Internet Applications)
- Tails-OS / Subgraph OS

Gehärtete Unixoide OS

- z.B. Trusted Solaris, bzw. Solaris Trusted Functionality, Trusted BSD, Hardened BSD, Hardened Linux
- Trusted Solaris Features sind jetzt im Standard Solaris 10 Release
  - Solaris ist Common Criteria EAL4+ zertifiziert
- TrustedBSD: gehärtetes FreeBSD
  - Access Control Lists, Audit (security event auditing), Extended Attributes, Mandatory Access Control Framework (MAC), Biba Integrity Policy, MLS Confidentiality Policy, Type Enforcement Policy (SEBSD)
- HardenedBSD
  - Address Space Layout Randomization (ASLR), mprotect hardening, Position Independent Executable (PIE) support, and PTrace hardening
- Einige mehr: Hardened Linux, Immunix
- Evtl. 2 Themen:
  - Sicherheit durch Modelle und Frameworks
  - Sicherheit durch technische Maßnahmen und Optimierungen

Sicherheit in Windows

- Windows ist in verschiedenen Versionen CC EAL4 zertifiziert
  - Auch Windows XP!
- Grund liegt u.a. in der Betriebssystem-Architektur
  - Security Manager
- Thema sollte das Sicherheitsmodell in Windows-Architektur beleuchten

Beweisbare Sicherheit

- Beweisbare Sicherheit ist der stärkste Beleg für Sicherheitseigenschaften
- Problem: Komplexität der zu betrachtenden Softwaresysteme
- Ansätze für Beweisbarkeit bestimmter Eigenschaften in Mikrokernel-Systemen
  - seL4: Beweisbare Kernel-Spezifikation
- Andere Beispiele: keyKOS, EROS (The Extremely Reliable Operating System)

Blockchain-Technologie

- Blockchain: kontinuierlich fortentwickelte, kryptographische Datenstruktur zur Notarisierung von Transaktionen im Bitcoin-Netzwerk
  - Dezentral
  - Einsatz von Proof-of-work
- Neue Anwendungsgebiete der Blockchain-Technologie
  - Smart Contracts
  - Digital Notary / Timestamping