Vorlesung

Systemsicherheit

Winter 2010/11

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

A Einführung

A.1 Motivation

- Ziele von Sicherheit im Betriebssystem
  - Datenvertraulichkeit
  - Datenintegrität
  - Systemverfügbarkeit
  - Verbindlichkeit
- Bedrohungen
  - Aufdeckung
  - Manipulation
  - Denial-of-Service
- Angreifer
  - Personen
  - Software
- Beabsichtigte und unbeabsichtigte Schädigung des Systems

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

A.2 Literatur

wird in den folgenden Kapiteln ergänzt

Eck08. Claudia Eckert. *IT-Sicherheit. Konzepte, Verfahren, Protokolle*. Oldenbourg, München, 5. Auflage, 2008.

Schn04. Bruce Schneier. *Secrets and Lies*. dpunkt-Verlag, Heidelberg, 2004.

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

A.3 Grundbegriffe

- Information
  - abstrakter Begriff
  - Darstellung, Speicherung: Daten(objekte)
  - Übertragung: Informationskanäle (legitim, verdeckt)
  - Zugriff, Bearbeitung: Subjekte
- Sicherheit
  - **Safety** (Funktionssicherheit)
    ein System funktioniert unter allen Betriebsbedingungen so wie es soll
  - **Security** (Informationssicherheit)
    Informationen können nicht unberechtigt gewonnen oder verändert werden
  - **Protection** (Datensicherheit)
    Schutz der Daten und Systemressourcen vor unberechtigtem Zugriff und Verlust
  - **Privacy** (Datenschutz, rechtlich gesehen)
    Kontrolle der Weitergabe von Informationen über Personen

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

A.4 Schwachstellen, Bedrohungen, Angriffe

- Schwachstellen (weaknesses) und Verwundbarkeit (vulnerability)
- Gefährdungsfaktoren
- Bedrohungen (threats)
  - Nutzung von Schwachstellen oder Verwundbarkeiten gegen Schutzziele
  - kann, aber muss nicht kritisch sein
- Risiko (risk)
  - Bewertung der Wahrscheinlichkeit von Schadensereignissen und der Auswirkungen
- Angriff (attack)
  - passiv: gegen Vertraulichkeit
  - aktiv: gegen Datenintegrität
- Angreifer
  - Hacker, Cracker, Skript Kiddies, Spione

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

B Vorlesungsüberblick

- Authentisierungskonzepte
- Schutzkonzepte, Autorisierung, Zugriffskontrolle
  - Objektschutz-Konzepte
    - Access Control Lists
    - Capabilities
  - Schutz von Dateien
    - Zugriffskontrolle in UNIX und Windows
    - Verschlüsselung von Dateien
  - Sichere Systemarchitekturen: Trusted Computing
- Angriffskonzepte, Systemschwachstellen
  - Trojaner, Würmer, privilegierte Anwendungen (s-Bit-Problem)
  - Angriffe von innerhalb / außerhalb des Systems

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

B Vorlesungsüberblick (2)

- Sicherheit von Programmen / Anwendungen
  - Sicherheitsprobleme bei der Ausführung von Anwendungen
    - Exploits (Pufferüberläufe etc.)
    - Return-oriented Programming
    - Mobiler Code
- Sicherheitskonzepte für die Ausführung von Anwendungen
  - Sprachbasierter Schutz (Typisierung)
  - Schutz durch die Laufzeitumgebung (Sandboxing, Proofs, Bsp. Java)
  - Sicherheitskonzepte in Betriebssystemen (Symbian, Linux, ...)
  - Unterstützung durch Entwicklungswerkzeuge
    (z.B. Vermeidung von Buffer-Overflows)
- Sicherheitsmodelle, Bewertungskriterien

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.