IT-Sicherheit

- Sicherheit vernetzter Systeme -

Prof. Dr. H.-G. Hegering, Dr. H. Reiser

Zeit: Montags, 14:15 – 15:45
*
Ort: Oettingenstr. 67, Raum 1.27

Inhaltsübersicht

1. Einleitung
   - Internet Worm versus Slammer
2. Grundlagen
   - OSI Security Architecture und Sicherheitsmanagement
   - Begriffsbildung
   - Security versus Safety
3. Security Engineering
   - Vorgehensmodell: Bedrohungs-/Risikoanalyse
   - Sicherheitsprobleme: Handelnde Personen, Notationen
   - Bedrohungen (Threats), Angriffe (Attacks), Schwächen (Vulnerabilities), z.B.:
     - Denial of Service
     - Malicious Code
     - Hoax, SPAM
     - Mobile Code
     - Buffer Overflow
     - Account / Password Cracking
     - Hintertüren / Falltüren
     - Rootkits
     - Sniffer
     - Port Scanner
   - Twenty Most Vulnerabilities
   - Sicherheitsanforderungen
4. Kryptologie, Grundlagen
   - Terminologie, Notationen
   - Steganographie
   - Kryptographie
     - Symmetrische Algorithmen
     - Asymmetrische Algorithmem
     - Hybride Kryptosysteme
     - One-Way- u. Hash-Funktionen

Innhaltsübersicht (2)

4. Kryptologie (Forts.)
   - Kryptoanalyse
     - Angriffe geg. Kryptosysteme
     - Schlüssellängen, Schlüsselsicherheit
5. Sicherheitsmechanismen
   - Identifikation
   - Authentisierung
   - Autorisierung und Zugriffskontrolle
   - Integritätssicherung
   - Vertraulichkeit
6. Netzwerk Sicherheit
   - Sicherheit der TCP/IP Protokollfamilie
   - IPSec
   - Firewall-Arten
   - Firewall-Architekturen

- Was ist nicht Gegenstand dieser Vorlesung?
  - Fortgeschrittene kryptographische Konzepte ⇒Kryptographie Vorlesung
  - Formale Sicherheitsmodelle und Sicherheitsbeweise

Einordnung der Vorlesung

- Bereich
  - LMU: Systemnahe und technische Informatik (ST), Anwendungen der Informatik (A)
  - TU: Informatik II (Wahlvorlesung)
- Hörerkreis
  - Informatik (Haupt- oder Nebenfach)
  - Vordiplom
- Voraussetzungen
  - Grundlegende Kenntnisse der Informatik
  - Rechnernetze (wünschenswert und hilfreich)
- Relevanz für Hauptdiplomsprüfung
  - LMU: Vorlesung mit 2 SWS **ohne** Übungsschein
  - TU: Wahlvorlesung vertiefend
  - Bachelor: 3 ECTS Punkte (vorrauss. mündliche Prüfung bei Prof. Hegering)

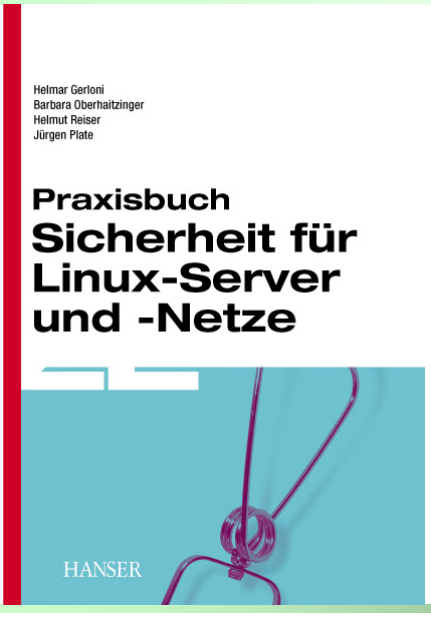
Termine und Organisation

- Vorlesungstermine und Raum:
  - Montags von 14:15 – 15:45
  - Raum 1.27
- Skript:
  - Kopien der Folien (pdf) zum Dowload
  - http://www.nm.ifi.lmu.de/Vorlesungen/itsec.shtml
- Kontakt:
  Helmut Reiser reiser@informatik.uni-muenchen.de
  Raum D0.3
- Sprechstunde:
  Montags 16:00 bis 17:00

Literatur: IT-Sicherheit

- Claudia Eckert
  IT-Sicherheit
  3. Auflage,
  Oldenbourg-Verlag, 2004
  ISBN 3-486-27205-5
  59,80 €

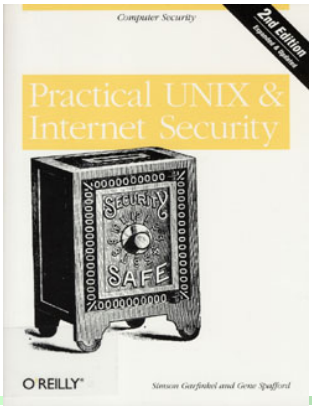
Literatur: IT-Sicherheit



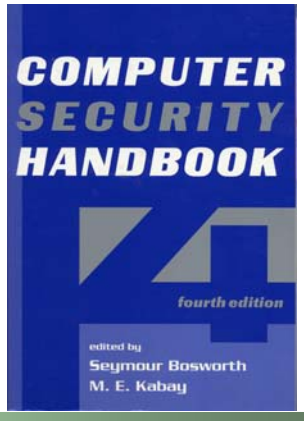
- Helmar Gerloni, Barbara Oberhaitzinger, Helmut Reiser, Jürgen Plate
  Praxisbuch Sicherheit für Linux-Server und -Netze
  Hanser-Verlag, 2004
  ISBN 3-446-22626-5
  34,90 €

Literatur: IT-Sicherheit

- Simson Garfikel, Gene Spafford
  Practical Unix & Internet Security
  O'Reilly, 1996
  ISBN 1-56592-148-8
  45 € - 60 €

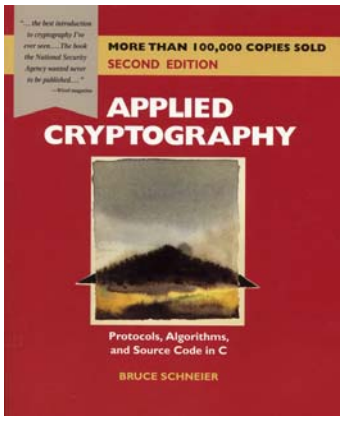


- Seymour Bosworth, M.E. Kabay
  Computer Security Handbook
  John Willey & Sons, 2002
  ISBN 0-471-41258-9
  75 $

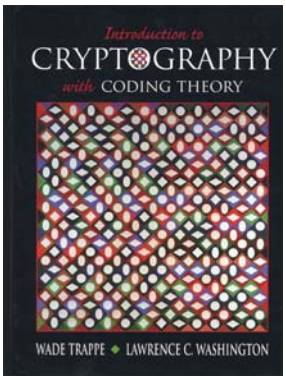


Literatur: Kryptologie

- Bruce Schneier
  Applied Cryptography
  John Willey & Sons, 1996
  ISBN 0-471-11709-9
  69 €

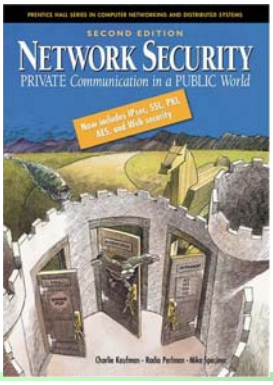


- Wade Trappe, Lawrence C. Washington
  Introduction to Cryptography with Coding Theory
  Prentice Hall, 2002
  ISBN 0-13-061814-4
  ca. 100 $

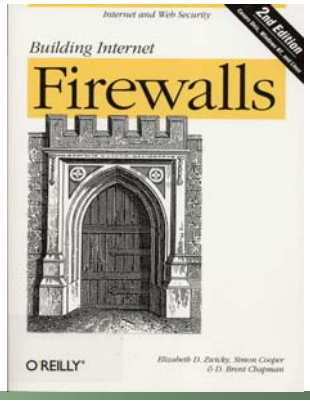


Literatur: Firewalls, Netzsicherheit

- Charly Kaufman, Radia Perlman, Mike Speciner
  Network Security, 2nd Ed.
  Prentice Hall, 2002
  ISBN 0-13-046019-2
  ca. 55 $



- Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman
  Building Internet Firewalls
  O'Reilly, 2002
  ISBN 1-56592-871-7
  ca. 45 $



Literaturliste

- Eine umfangreichere Literaturliste wird im Web zur Verfügung gestellt:

  `www.nm.ifi.lmu.de/Vorlesungen/itsec.shtml`

Weitere Veranstaltungen in diesem Semester

- Vorlesungen:
  - Netz- und Systemmanagement, (Prof. Dr. Hegering)
    Freitag 8:15 – 11:00, Raum N1190 (TUM)
    `www.nm.ifi.lmu.de/Vorlesungen/nsmgmt.shtml`
  - Design und Realisierung von E-Business und Internet-Anwendungen
    (Dr. M. Nerb, Dr. S. Heilbronner, Dr. I. Radisic, Dr. K. Bönisch)
    Donnerstag 16:15 – 17:45, Raum E52 (Theresienstrasse)
    `www.nm.ifi.lmu.de/Vorlesungen/ecpm.shtml`
- Praktika:
  - Praktikum IT-Sicherheit (Prof. Dr. Hegering, W. Hommel, Dr. H. Reiser)
    `www.nm.ifi.lmu.de/Praktika/secp.shtml`
  - Praktikum Rechnernetze (Prof. Dr. Hegering, M. Brenner, V. Danciu)
    `www.nm.ifi.lmu.de/Praktika/rnp.shtml`

Weitere Veranstaltungen in diesem Semester (2)

- Hauptseminar:
  - Grid Computing: Auf dem Weg zu einer neuen globalen Infrastruktur !?
    (Prof. Dr. Hegering)
    Blockveranstaltung mit externen Vorträgen
  - www.nm.ifi.lmu.de/Hauptseminare/ss05/
- Diplomarbeiten:
  www.nm.ifi.lmu.de/da.shtml
- Fortgeschrittenenpraktika, Systementwicklungsprojekte
  www.nm.ifi.lmu.de/fopra.shtml