IT-Sicherheit

- Sicherheit vernetzter Systeme -

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

Zeit: Mittwochs, 16:15 – 17:45

*

Ort: Oettingenstr. 67, Raum 0.37

Inhaltsübersicht

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-Architekturen
   - Praktische Beispiele aus dem LRZ

- 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: Modul IN2101
- Hörerkreis
  - Informatik (Haupt- oder Nebenfach)
  - TU: Informatik (Bachelor, Master, Diplom), Wahlfach
  - TU: Angewandte Informatik (Master), Wahlfach empfehlenswert
- Voraussetzungen
  - Grundlegende Kenntnisse der Informatik
  - Rechnernetze (wünschenswert und hilfreich)
- Relevanz für Hauptdiplomsprüfung
  - LMU: Vorlesung mit 2 SWS **ohne** Übungsschein
  - TU: Wahlvorlesung vertiefend
  - Credits: 3 ECTS Punkte (Prüfung mündlich oder schriftlich)

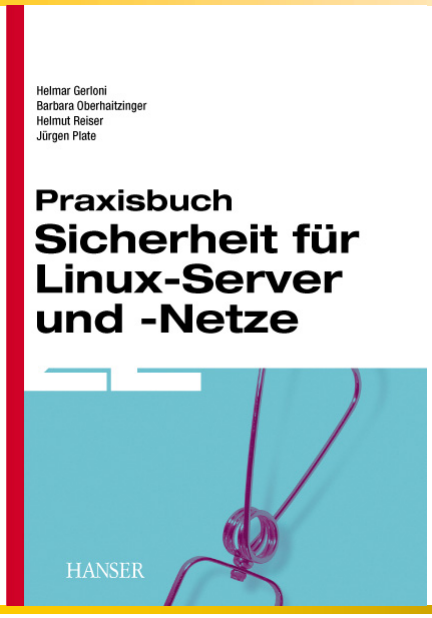
Termine und Organisation

- Vorlesungstermine und Raum:
  - Mittwochs von 16:15 – 17:45
  - Raum 0.37
- Skript:
  - Kopien der Folien (pdf) zum Dowload
  - http://www.nm.ifi.lmu.de/itsec
- Kontakt:
  Helmut Reiser reiser@lrz.de
  LRZ: Boltzmannstr. 1, 85748 Garching
- Raum I.2.070
- Sprechstunde:
  Montags 13:00 bis 14:00 im LRZ; nach der Vorlesung oder nach Vereinbarung

Literatur: IT-Sicherheit

- Claudia Eckert
  IT-Sicherheit
  4. Auflage,
  Oldenbourg-Verlag, 2006
  ISBN 3486578510
  59,80 €

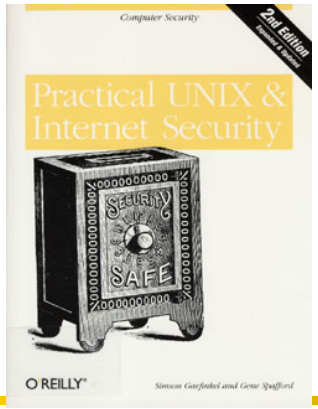
Literatur: IT-Sicherheit



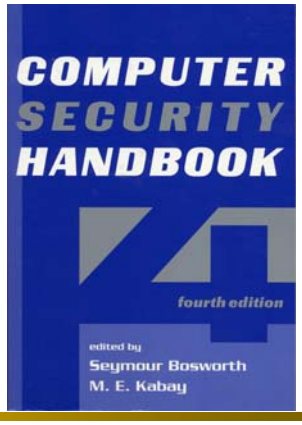
- Helmar Gerloni, Barbara Oberhaitzinger, Helmut Reiser, Jürgen Plate
  Praxisbuch Sicherheit für Linux-Server und -Netze
  Hanser-Verlag, 2004
  ISBN 3-446-22626-5
  34,90 €

Literatur: IT-Sicherheit

- Simson Garfikel, Gene Spafford
  Practical Unix & Internet Security
  O'Reilly, 2003
  ISBN 0596003234
  ca. 50 €

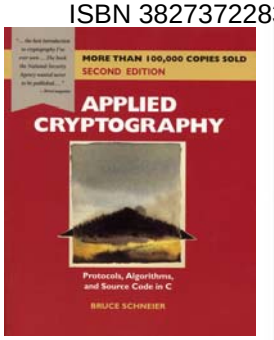


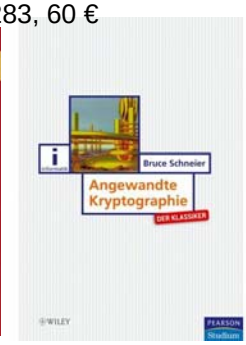
- Seymour Bosworth, M.E. Kabay
  Computer Security Handbook
  John Willey & Sons, 2003
  ISBN 0-471-41258-9
  ca. 90 – 100 €



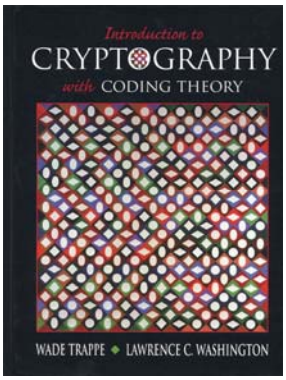
Literatur: Kryptologie

- Bruce Schneier
  Applied Cryptography
  John Willey & Sons, 1996
  ISBN 0-471-11709-9
  69 €
  Angewandte Kryptographie
  Pearson Studium, 2005
  ISBN 3827372283, 60 €



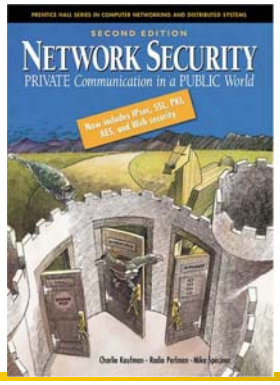


- Wade Trappe, Lawrence C. Washington
  Introduction to Cryptography with Coding Theory
  Prentice Hall, 2002
  ISBN 0-13-061814-4
  ca. 100 $

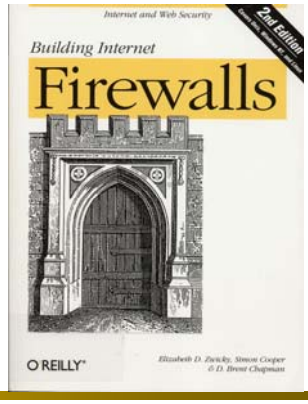


Literatur: Firewalls, Netzsicherheit

- 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. 50 €



Literaturliste

- Eine umfangreichere Literaturliste wird im Web zur Verfügung gestellt:

  www.nm.ifi.lmu.de/itsec

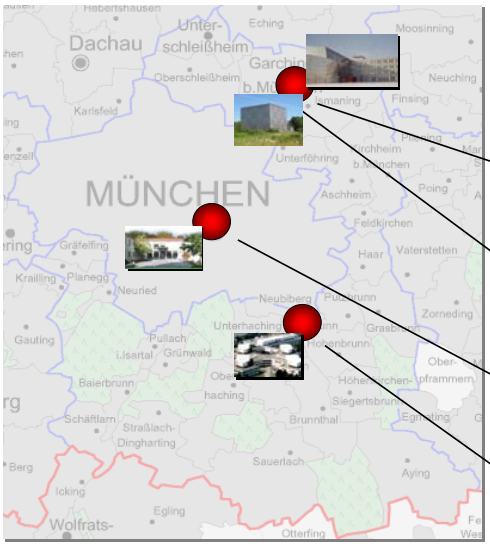
Weitere Veranstaltungen in diesem Semester

- Vorlesungen:
  - Rechnernetze, (Prof. Dr. Hegering)
    Freitag 8:15 – 11:00, Raum N1190 (TUM) und 00.08.038 (Garching)
    www.nm.ifi.lmu.de/rn
  - Komponenten zum Aufbau von Rechnernetzen (Dr. M. Garschhammer, Prof. Dr. Hegering)
    Donnerstag 8:15 – 11:00, Raum B132 (Theresienstrasse)
    www.nm.ifi.lmu.de/comp
- Praktika:
  - Praktikum IT-Sicherheit (Prof. Dr. Hegering, N. Felde, W. Hommel, Dr. H. Reiser, M. Yampolskiy)
    www.nm.ifi.lmu.de/secp
  - Rechnerbetriebspraktikum (Prof. Dr. Hegering, Dr. E. Bötsch, Dr. P. Eilfeld)
    www.nm.ifi.lmu.de/rbp

Weitere Veranstaltungen in diesem Semester (2)

- Kompaktseminar:
  - Prozessorientiertes IT-Service Management anhand von Unternehmensplanspielen (Prof. Dr. Hegering, R. Kuhlig, M. Brenner, T. Schaaf)
    Blockveranstaltung
  - www.nm.ifi.lmu.de/teaching/LMU/Seminare/2006ws/itsm/
- Diplomarbeiten:
  www.nm.ifi.lmu.de/da.shtml
- Fortgeschrittenenpraktika, Systementwicklungsprojekte
  www.nm.ifi.lmu.de/fopra.shtml

Forschung: MNM Team



MNM TEAM
Munich Network Management Team

LMU

der Bundeswehr Universität München