IT-Sicherheit

- Sicherheit vernetzter Systeme -

Dr. Helmut Reiser

Zeit: Montags, 15:15 – 17:45

Ort: Oettingenstr. 67, Raum 1.27

Inhaltsübersicht

Innhaltsübersicht (2)

6. Asymmetrische und Hybride Kryptosysteme
   - RSA
   - Schlüssellängen und Schlüsselsicherheit
   - Hybride Systeme
   - Digitale Signatur
7. Kryptographische Hash Funktionen
   - Konstruktion von Hash-Fkt.
   - Angriffe auf Hash-Fkt.
   - MD4, MD5
   - Whirlpool Hashing
8. Sicherheitsmechanismen
   - Vertraulichkeit
   - Integrität
   - Identifikation
   - Authentisierung
   - Autorisierung und Zugriffskontrolle
9. Netz Sicherheit - Schicht 2: Data Link Layer
   - Point-to-Point Protocol (PPP)
   - Point-to-Point Tunneling Protocol (PPTP)
   - Layer 2 Tunneling Protocol (L2TP)
   - IEEE 802.1x
10. Schicht 3: Network Layer
    - IP Gefahren und Schwächen
    - IPSec
    - Schlüsselverteilung mit IKE

Innhaltsübersicht (3)

11. Schicht 4 - Transport Layer
    - TCP / UDP
    - Secure Socket Layer / Transport Layer Security (SSL/TLS)
12. WLAN Sicherheit
    - WEP
    - WPA
13. Firewall-Architekturen
15. Sicherheitsmechanismen der Anwendungsschicht
    - Secure Shell (ssh)
16. Anti-Spam Maßnahmen
17. Beispiele aus der Praxis (LRZ)

- Was ist nicht Gegenstand dieser Vorlesung
  - Fortgeschrittenen krytographische Konzepte ⇒ Vorlesung Kryptologie
  - Formale Sicherheitsmodelle und Sicherheitsbeweise

Einordnung der Vorlesung

- Bereich
  - Systemnahe und technische Informatik (ST), Anwendungen der Informatik (A)
- Hörerkreis (LMU)
  - Informatik Diplom
  - Informatik Master
  - Informatik Bachelor („Vertiefende Themen der Informatik für Bachelor“)
- Voraussetzungen
  - Grundlegende Kenntnisse der Informatik
  - Rechnernetze (wünschenswert und hilfreich)
- Relevanz für Hauptdiplomsprüfung
  - Vorlesung plus Übung: 3 + 2 SWS
  - Credits: 6 ECTS Punkte

Termine und Organisation

- Vorlesungstermine und Raum:
  - Montags von 15:15 – 17:45, Raum Oe 1.27
- Übung; Beginn 29.10.
  - Mittwochs von 14:15 - 15:45 in Oe 1.27
  - Übungsleitung:
    - Tobias Lindinger,lindinge@nm.ifi.lmu.de
    - Nils gentschen Felde, felde@nm.ifi.lmu.de
- 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 11:00 bis 12:00 im LRZ; nach der Vorlesung oder nach Vereinbarung

Schein

- Anmeldung zur **Übung** und Klausur
- Prüfung zum Erhalt des Scheins
- Notenbonus durch Hausaufgaben
  - Übungsblatt enthält Hausaufgabe
  - Hausaufgabe bei der Übung abgeben
  - Es werden 3 Blätter / Aufgaben gewählt und korrigiert

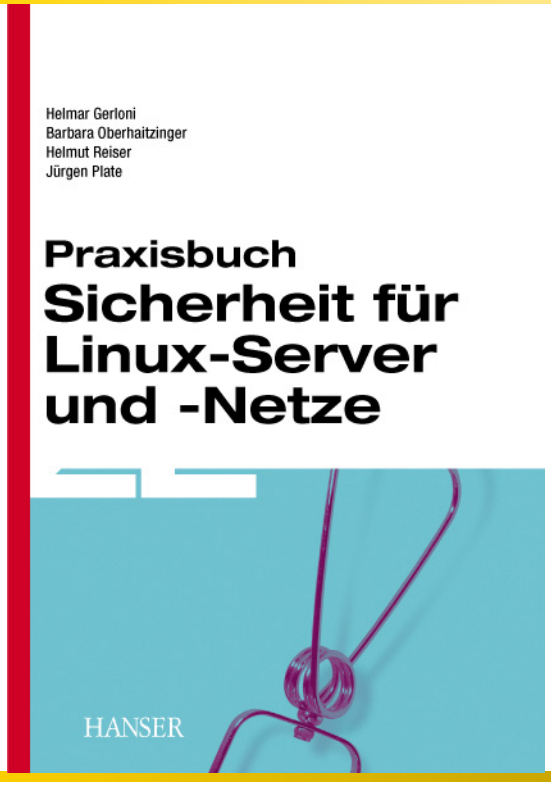
Anzahl korrekter Lösungen	Bonus	Beispiel
3	2 Stufen	Vorher: 3.0; Nachher: 2.3
2	1 Stufe	Vorher: 3.0; Nachher: 2.7
1	0 Stufen	Vorher: 3.0; Nachher: 3.0

- Bonussystem nur wirksam bei **bestandener** Prüfung

Literatur: IT-Sicherheit

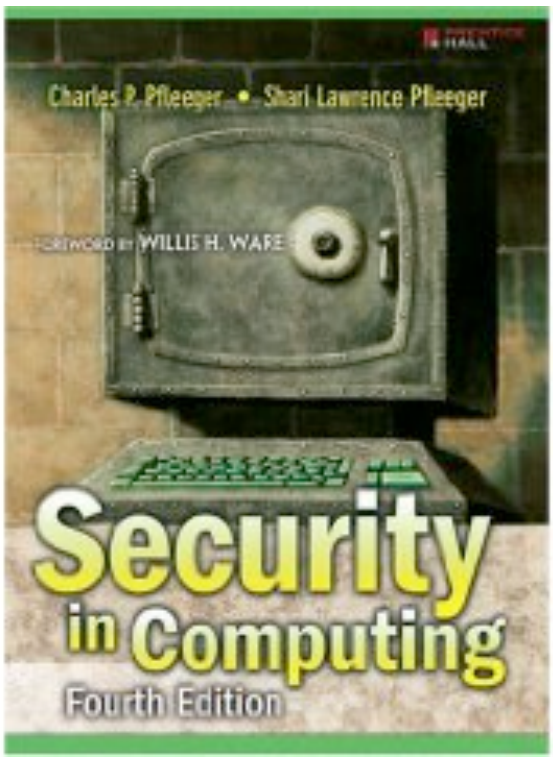
- Claudia Eckert
  IT-Sicherheit
  5. Auflage,
  Oldenbourg-Verlag, 2007
  ISBN 3486578510
  59,80 €

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 €

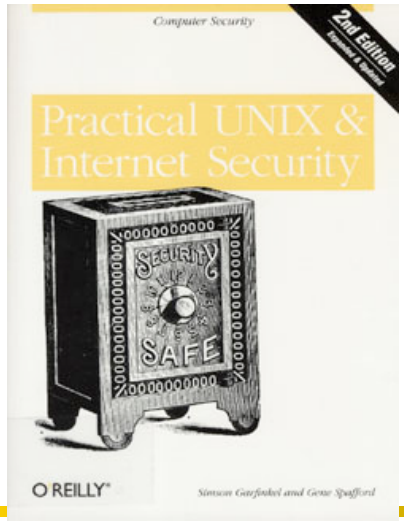
Literatur: IT-Sicherheit



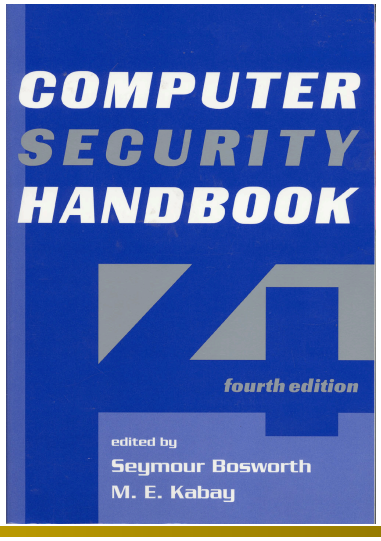
- Charles P. Pfleeger, Sharie L. Pfleeger
  Security in Computing
  4. Auflage,
  Pearson, 2006 / 2008
  ISBN 978-8120334151
  70 $

Literatur: IT-Sicherheit

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

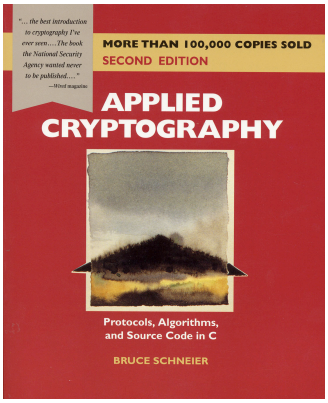


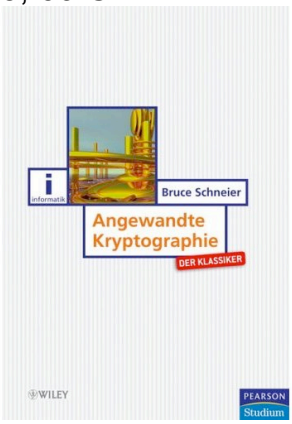
- Seymour Bosworth, M.E. Kabay
  Computer Security Handbook
  John Willey & Sons, 2003
  ISBN 0-471-41258-9
  ca. 90 – 100 €



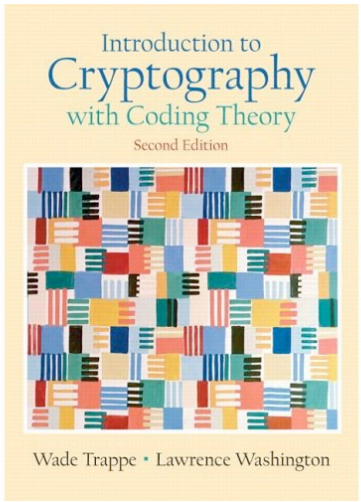
Literatur: Kryptologie

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



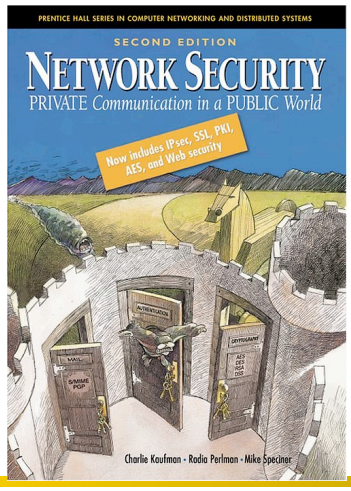


- Wade Trappe, Lawrence C. Washington
  Introduction to Cryptography with Coding Theory
  Prentice Hall, 2005
  ISBN 978-0131862395
  83 €

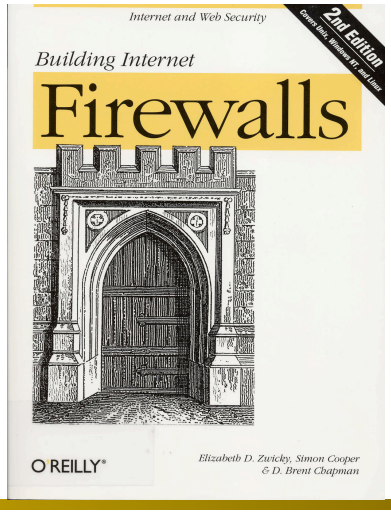


Literatur: Firewalls, Netzsicherheit

- Charly Kaufman, Radia Perlman, Mike Speciner
  Network Security, 2nd Ed.
  Prentice Hall, 2002
  ISBN 0-13-046019-2
  ca. 54 €



- 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`

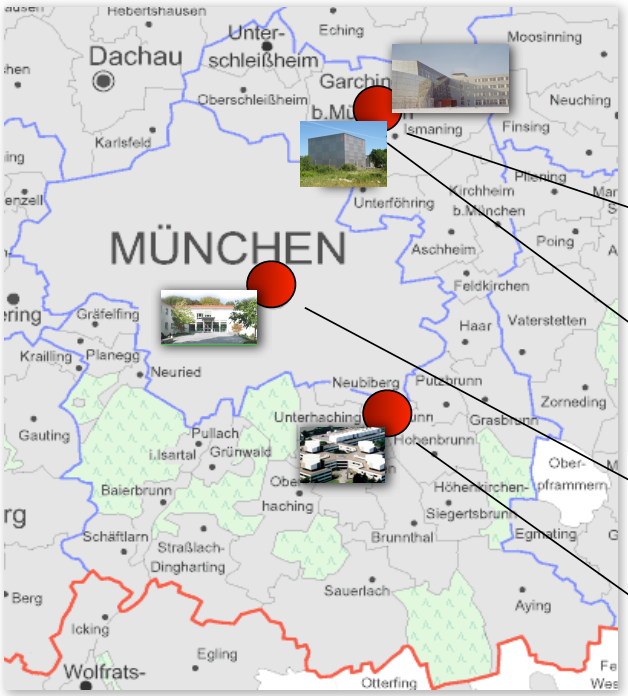
Weitere Veranstaltungen in diesem Semester

- Vorlesungen:
  - Rechnernetze, (Prof. Dr. Hegering, Prof. Dr. Kranzlmüller, Dr. V. Danciu)
    Freitag 11:15 – 14:00, LMU Hauptgebäude A140
    www.nm.ifi.lmu.de/rn
- Praktika:
  - Rechnerbetriebspraktikum (Prof. Dr. Hegering, Prof. Dr. Dreo-Rodosek (UniBW), Dr. E. Bötsch, V. Kokkas (LRZ)) www.nm.ifi.lmu.de/rbp
- Hauptseminar:
  - Sichere und integre IT-Systeme (Prof. Dr. Dreo-Rodosek (UniBW), Dr. Helmbrecht (BSI)), www.unibw.de/inf3/lehre/semi/sichht08/index_html
- Diplomarbeiten:

  www.nm.ifi.lmu.de/teaching/Auschreibungen/Diplomarbeiten
- Fortgeschrittenenpraktika, Systementwicklungsprojekte

  www.nm.ifi.lmu.de/teaching/Ausschreibungen/Fopras

Forschung: MNM Team



MNM TEAM
Munich Network Management Team

LMU

der Bundeswehr Universität München