

IT-Sicherheit

- Sicherheit vernetzter Systeme -

Dr. H. Reiser

Zeit: Montags, 16:15 – 17:45

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
4. Kryptologie, Grundlagen
 - Twenty Most Vulnerabilities
 - Sicherheitsanforderungen
 - Terminologie, Notationen
 - Steganographie
 - Kryptographie
 - Symmetrische Algorithmen
 - Asymmetrische Algorithmen
 - Hybride Kryptosysteme
 - One-Way- u. Hash-Funktionen



Inhaltsübersicht (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
- 7. 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 Hauptdiplomprüfung
 - LMU: Vorlesung mit 2 SWS **ohne** Übungsschein
 - TU: Wahlvorlesung vertiefend
 - Credits: 3 ECTS Punkte (Prüfung mündlich oder schriftlich)



Termine und Organisation

- Vorlesungstermine und Raum:
 - Montags von 16:15 – 17:45
 - Raum 1.27

- 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 Oberhaidinger
Helmut Reiser
Jürgen Plate

Praxisbuch Sicherheit für Linux-Server und -Netze



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



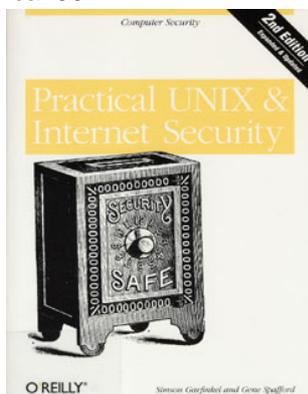
© Helmut Reiser, LRZ, WS 07/08

IT-Sicherheit

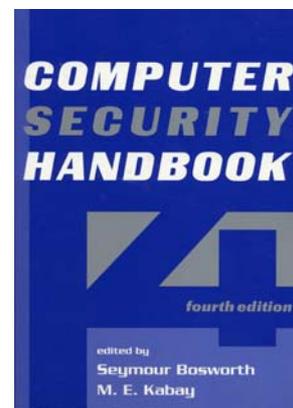
7

Literatur: IT-Sicherheit

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



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



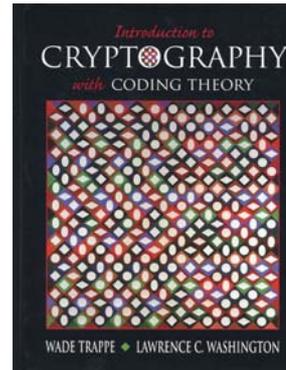
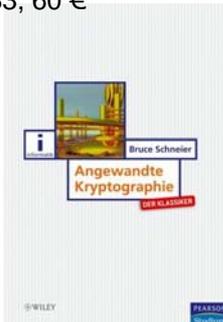
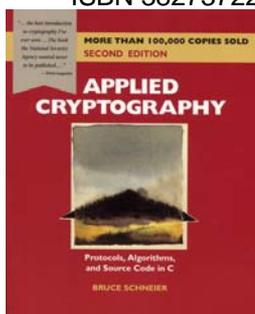
© Helmut Reiser, LRZ, WS 07/08

IT-Sicherheit

8

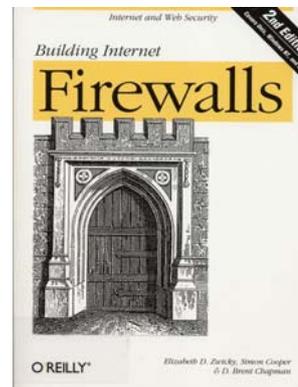
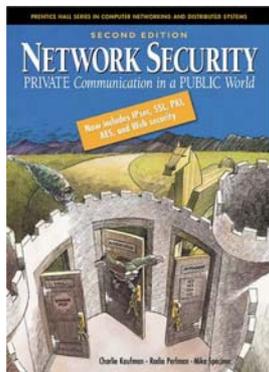
Literatur: Kryptologie

- Bruce Schneier
Applied Cryptography
John Wiley & 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, Dr. V. Danciu)
Freitag 8:15 – 11:00, Raum N1190 (TUM) und HE.009 (LRZ, Garching)
www.nm.ifi.lmu.de/rn
- Komponenten zum Aufbau von Rechnernetzen (Prof. Dr. Hegering, Dr. S. Graupner)
Blockveranstaltung; Termine: 07.12; 08.12; 14.12 und 15.12.
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, V. Kokkas)
www.nm.ifi.lmu.de/rbp

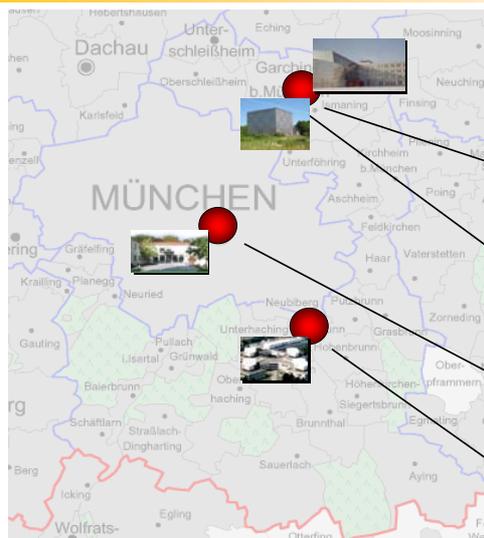


Weitere Veranstaltungen in diesem Semester (2)

- **Kompaktseminar:**
 - Prozessorientiertes IT-Service Management anhand von Unternehmensplanspielen (Prof. Dr. Hegering, R. Kuhlig, B. Gögetap, M. Brenner, T. Schaaf)
Blockveranstaltung: 10.-12.10.
www.nm.ifi.lmu.de/teaching/LMU/Seminare/2007ws/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



der Bundeswehr
Universität München



Seminar an der Uni der Bundeswehr

- Von der Sicherheit elektronischer Dokumente bis zu digitalen Identitäten
 - Seminarleiter ist Dr. Udo Helmbrecht (Präsident des BSI):
 - Grundlagen von Public-Key-Infrastrukturen (PKI)
 - Schutz elektronischer Dokumente (z.B. signieren von pdf-Dokumenten)
 - Grundlagen und Anwendungen der RFID-Technologie
 - RFIDs in Identitätsdokumenten
 - Zukünftige Anwendungen: Pervasive Computing
 - Termine:
 - 15.10. 15:00-16:00 Vorstellung und Vergaben der Themen
 - 19.11.Präsenzveranstaltung zur Diskussion der Themen
 - 14.12. / 17.12.Präsentation der Themen
 - http://www.unibw.de/inf3/lehre/semi/sichht07/index_html
 - Bei Interesse Mail an: gabi.dreo@unibw.de

