

IT-Sicherheit

- Sicherheit vernetzter Systeme -

Priv.-Doz. Dr. Helmut Reiser
Dr. Wolfgang Hommel

Zeit: Montags, 15:15 – 17:45

Ort: Geschwister-Scholl-Platz 1,
Hörsaal E 216

Inhaltsübersicht

1. Einleitung
 - ❑ Internet Worm versus Slammer
 - ❑ Stuxnet
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
 - ❑ Rechtliche Regelung: StGB
 - ❑ Top Cyber Security Risks
 - ❑ Sicherheitsanforderungen
5. Kryptologie, Grundlagen
 - ❑ Terminologie, Notationen
 - ❑ Steganographie
 - ❑ Kryptographie, Begriffe und Definitionen
 - ❑ Kryptoanalyse
5. Symmetrische Kryptosysteme
 - ❑ Data Encryption Standard (DES)
 - ❑ Advanced Encryption Std. (AES)

Inhaltsübersicht (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 2: WLAN Sicherheit

- WEP
- WPA
- WPA2

Inhaltsübersicht (3)

11. Schicht 3: Network Layer

- IP Gefahren und Schwächen
- IPSec
- Schlüsselverteilung mit IKE

12. Schicht 4 - Transport Layer

- TCP / UDP
- Secure Socket Layer / Transport Layer Security (SSL/TLS)

13. Schicht 7: Secure Shell (ssh)

- SSH v1 versus SSH v2
- Protokoll-Architektur

14. Firewalls und Intrusion Detection Systeme

- Firewall-Klassen
- Firewall-Architekturen
- IDS-Arten

15. Beispiele aus der Praxis (LRZ)

15. Anti-Spam Maßnahmen

16. Beispiele aus der Praxis des LRZ

- Struktur des MWN
- Virtuelle Firewalls
- Nat-O-Mat
- NYX

17. Datenschutz

- Persönlichkeitsrechte u. Datenschutz
- Datenspuren und Schutzmaßnahmen

⊙ Was ist nicht Gegenstand dieser Vorlesung

- Fortgeschrittenen kryptographische 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 E 216 (Geschwister-Scholl Pl. 1)
- Übung; Beginn 02.11.2011
 - Mittwochs von 14:15 - 15:45 in Raum C 113 (Theresienstr. 41)
 - Übungsleitung:
Stefan Metzger, metzger@lrz.de

- Skript:
 - Kopien der Folien (pdf) zum Dowload
 - <http://www.nm.ifi.lmu.de/itsec>

Videoaufzeichnung: videoonline.edu.lmu.de

- Kontakt:

Helmut Reiser	Wolfgang Hommel
reiser@lrz.de	hommel@lrz.de
LRZ, Raum I.2.070	LRZ, Raum I.2.074

- Sprechstunde:

Montags 11:00 bis 12:00 im LRZ; nach der Vorlesung oder nach



Schein

- Anmeldung zur **Übung** und Klausur
- Prüfung zum Erhalt des Scheins
- Notenbonus durch Hausaufgaben
 - Übungsblatt enthält Hausaufgabe
 - Hausaufgabe bei der Übung abgeben
 - Es werden 4 Blätter / Aufgaben gewählt und korrigiert

Anzahl korrekter Lösungen	Bonus	Beispiel
4	2 Stufen	Vorher: 3.0; Nachher: 2.3
2 oder 3	1 Stufe	Vorher: 3.0; Nachher: 2.7
1	0 Stufen	Vorher: 3.0; Nachher: 3.0

- Bonussystem nur wirksam bei **bestandener** Prüfung
- Beste Note 1.0
- **Keine** Nachholklausur

Literatur: IT-Sicherheit



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

Literatur: IT-Sicherheit

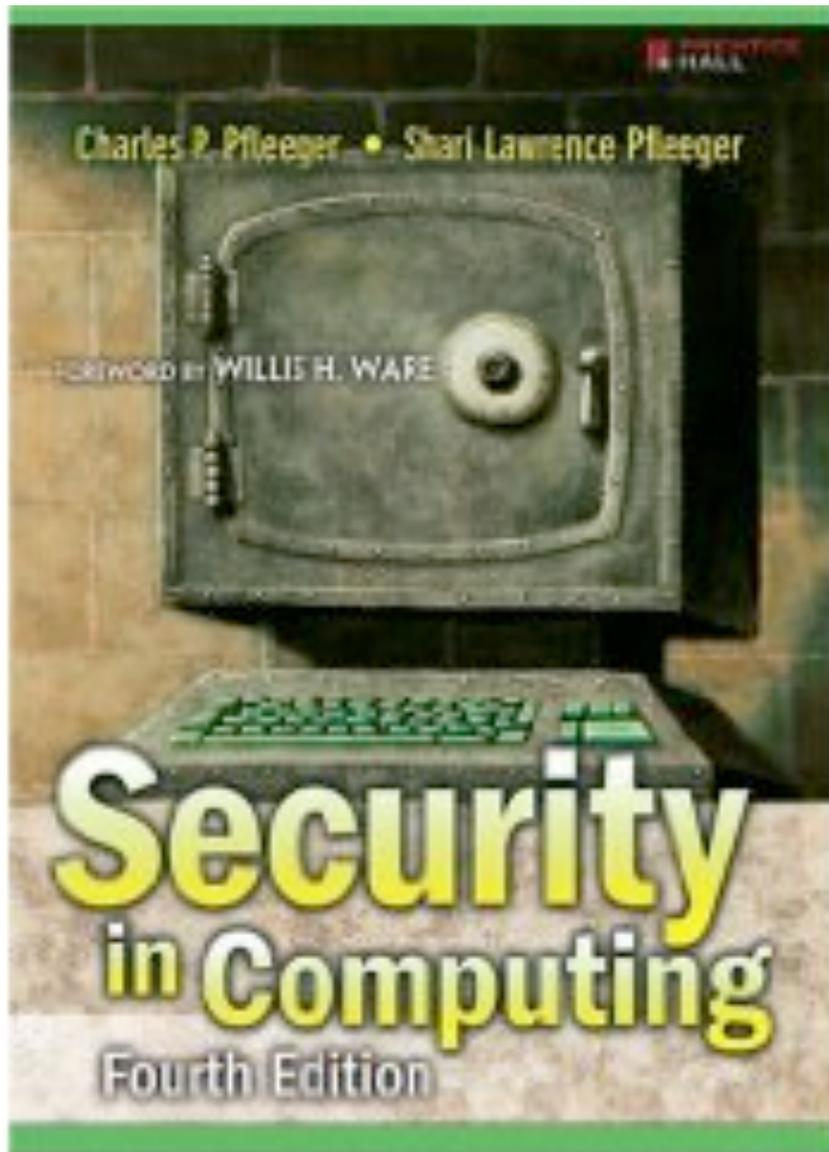
Helmar Gerloni
Barbara Oberhaidinger
Helmut Reiser
Jürgen Plate

Praxisbuch Sicherheit für Linux-Server und -Netze

HANSER

- 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 €

Literatur: IT-Sicherheit



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

Literatur: IT-Sicherheit



Brenner M., Gentschen Felde, N.,
Hommel, W., Metzger, S., Reiser, H.,
SchAAF, T.

Praxisbuch ISO/IEC 27001 - Management der Informationssicherheit und Vorbereitung auf die Zertifizierung

Hanser, 2011

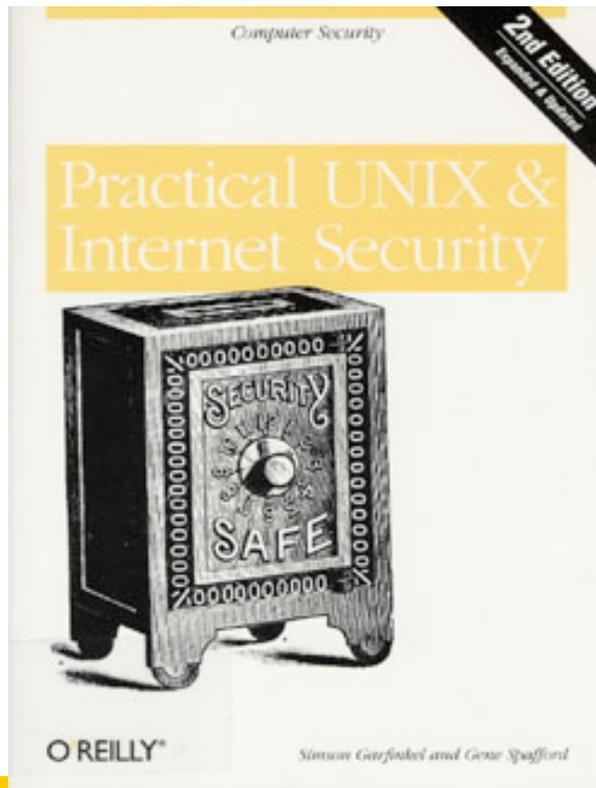
ISBN-10: 3-446-43026-1

ISBN-13: 978-3-446-43026-6

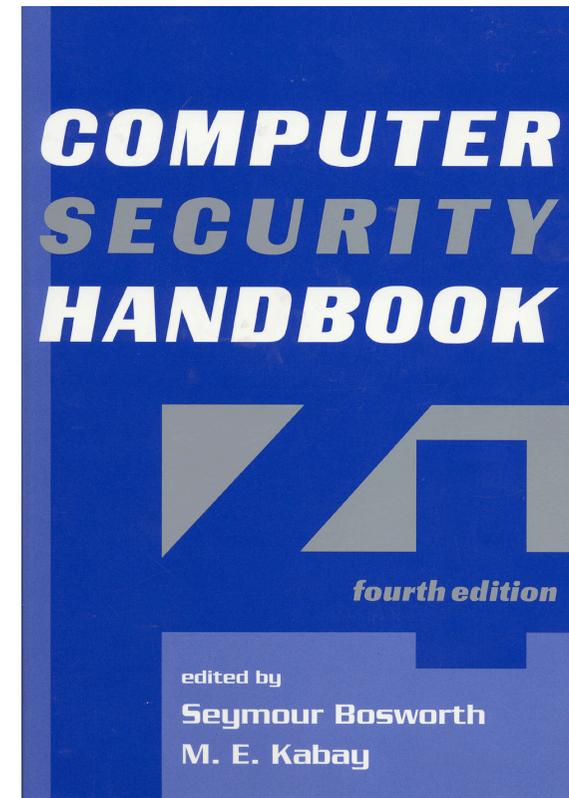
59,90 €

Literatur: IT-Sicherheit

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

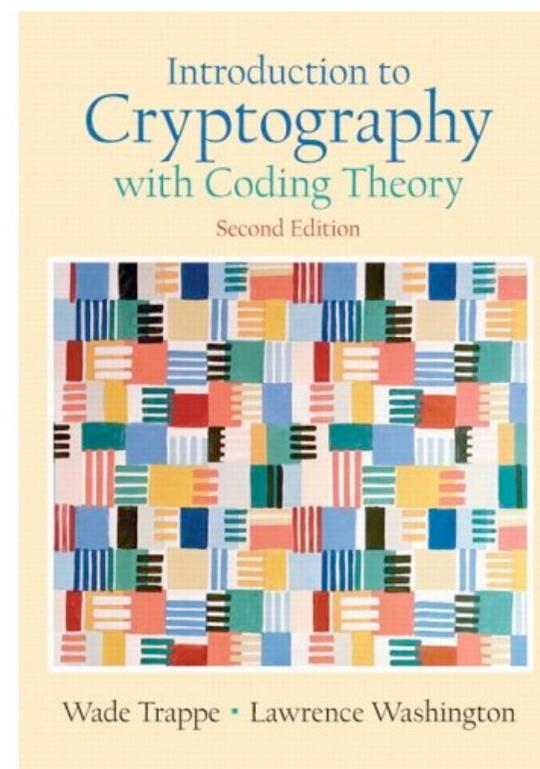
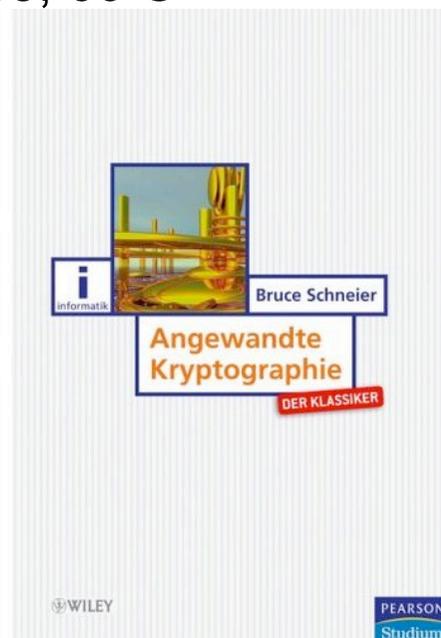
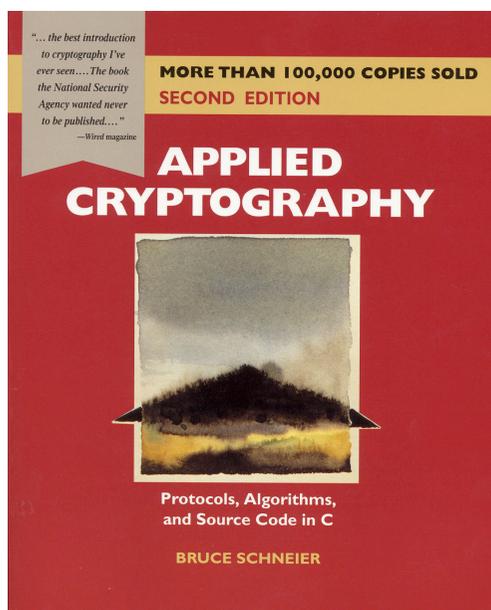


- Seymour Bosworth, M.E. Kabay
Computer Security Handbook
John Wiley & Sons, 2003
ISBN 0-471-41258-9
ca. 90 – 100 €



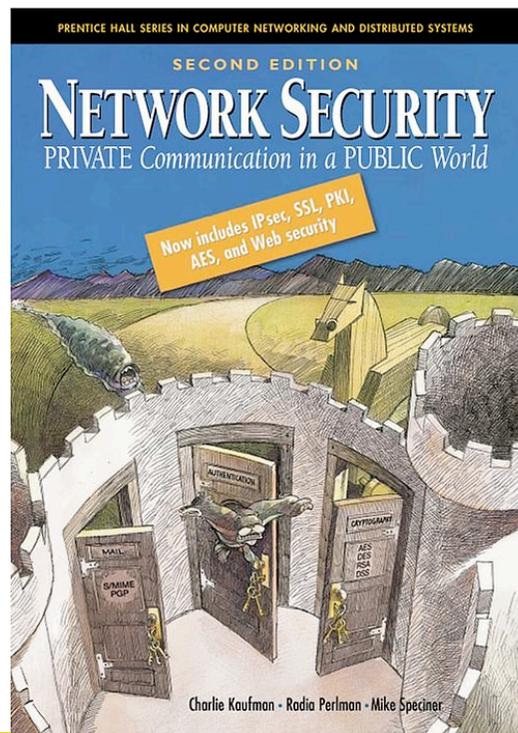
Literatur: Kryptologie

- 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 €

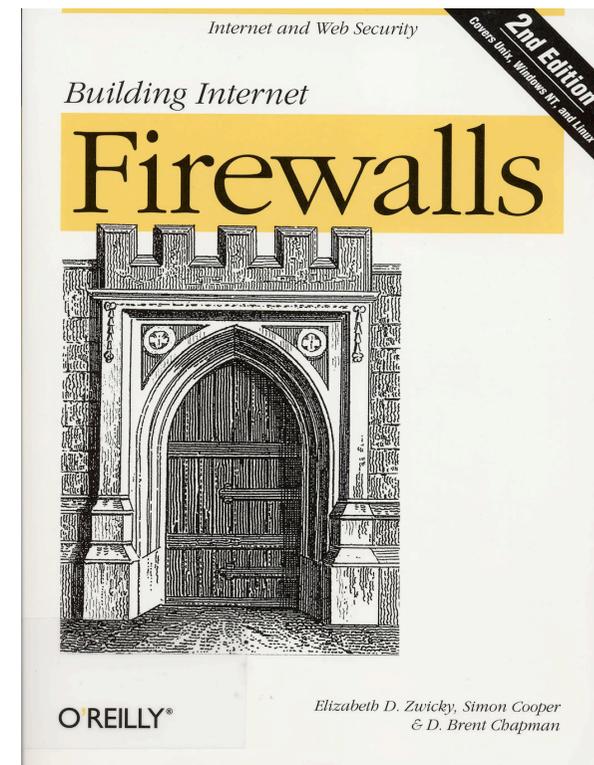


Literatur: Firewalls, Netzsicherheit

- 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 €



Weitere Veranstaltungen in diesem Semester

■ Vorlesungen:

- Parallel Computing: Grundlagen und Anwendungen (Prof. Dr. Kranzlmüller, Dr. K. Furlinger, C. Klausecker)
Freitags 9:00 – 12:00, Oettingenstr. 67, L 155
www.nm.ifi.lmu.de/parallel/

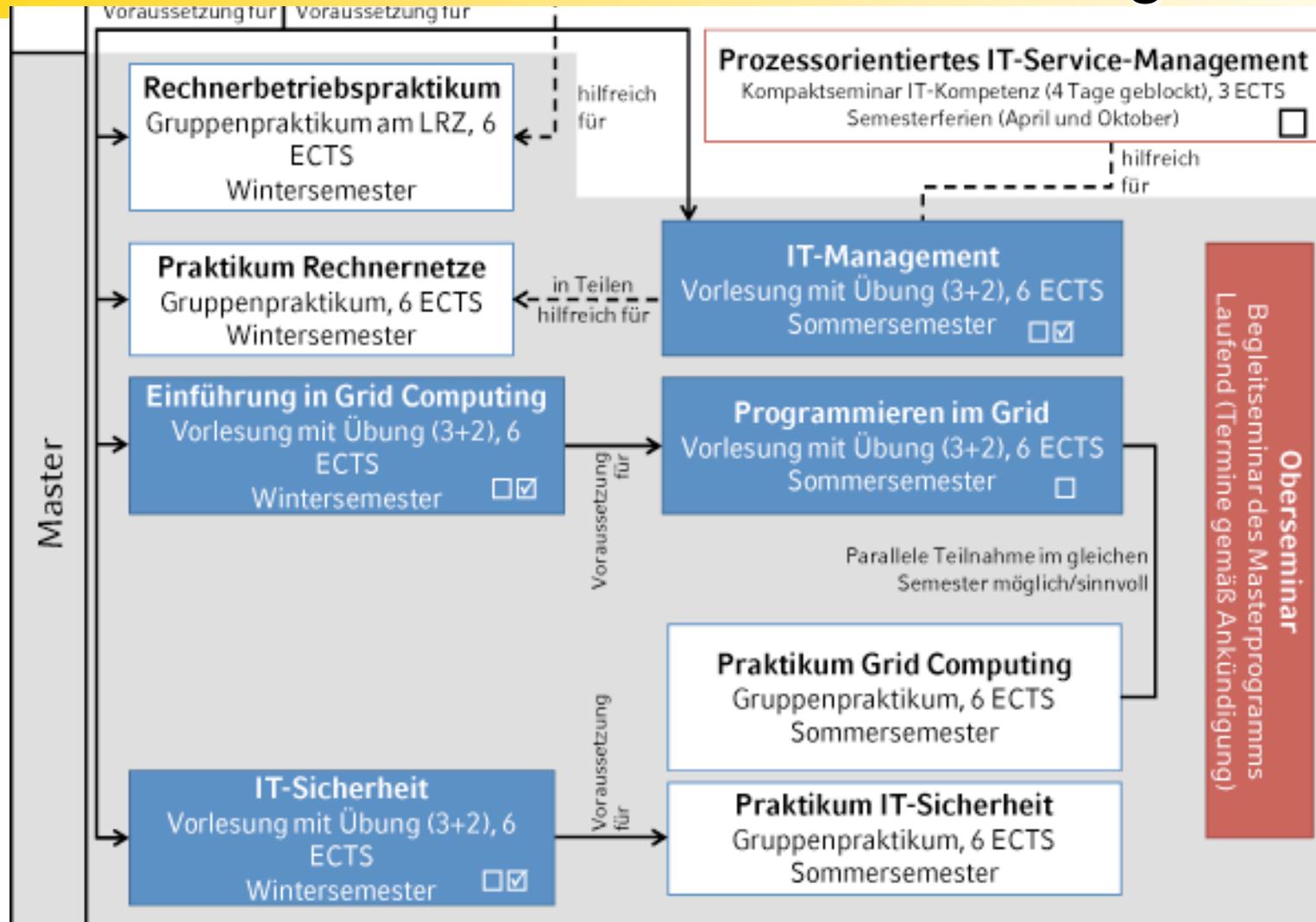
■ Praktika:

- Rechnernetze (Prof. Dr. Kranzlmüller, Prof. Dr. Hegering, Dr. V. Danciu, M. Metzker) www.nm.ifi.lmu.de/rnp
- Rechnerbetriebspraktikum (Prof. Dr. Kranzlmüller, Prof. Dr. Hegering, Dr. Bötsch, V. Kokkas)
www.lrz.de/services/schulung/rbp/

■ Seminar:

- Wissenschaftliches Arbeiten und Lehren (Pro. Dr. Kranzlmüller, Dr. M. Schiffers, S. Ferlin Oliveira)

Übersicht über Lehrveranstaltungen



- | | | | | | |
|---|-----------|---|---|-------------------------------------|---------------------------------------|
|  | Vorlesung |  | Informatik-Seminar | <input type="checkbox"/> | Wahlpflichtveranstaltung |
|  | Praktikum |  | Seminar zu überfachlichen Grundlagen (IT-Kompetenz) | <input checked="" type="checkbox"/> | Pflichtveranstaltung |
| | | | | <input checked="" type="checkbox"/> | Verwendbar als Vertiefende Themen der |

Weitere Veranstaltungen in diesem Semester

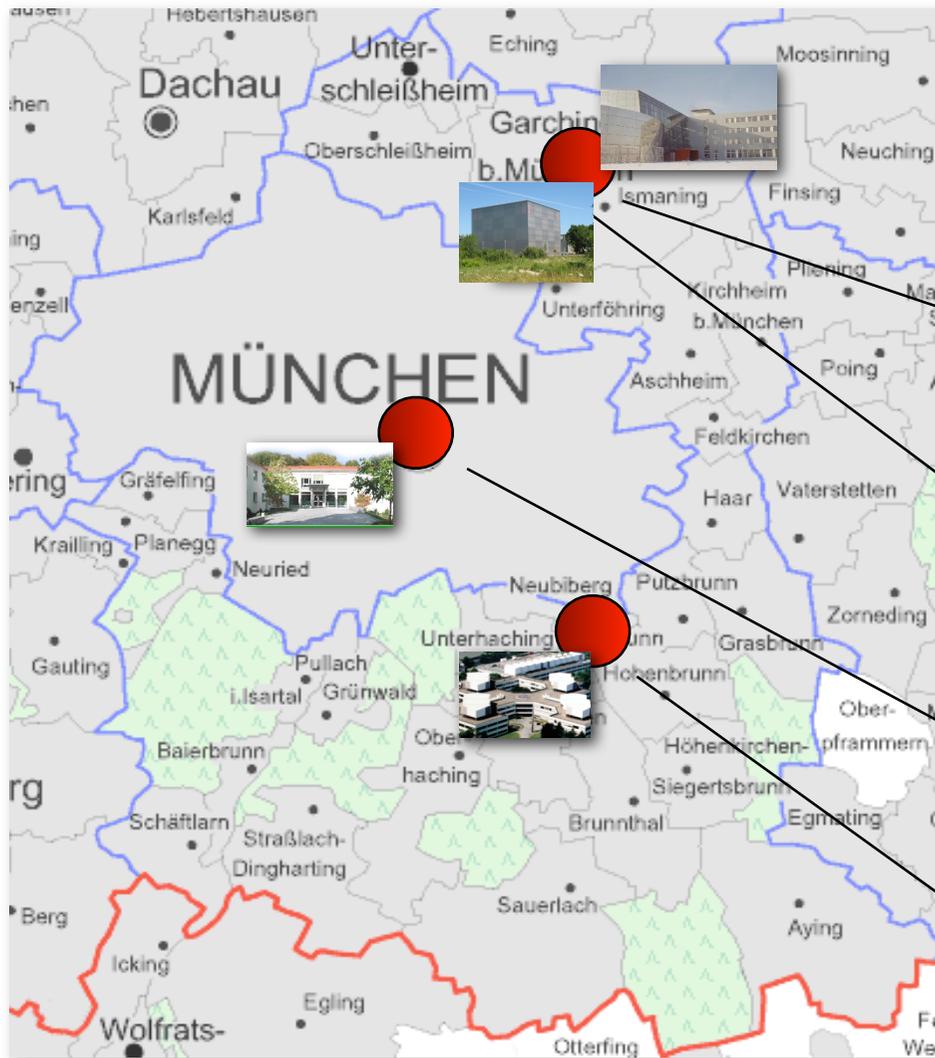
- Master und Diplomarbeiten:

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

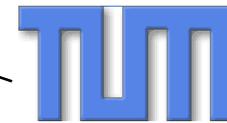
- Fortgeschrittenenpraktika, Systementwicklungsprojekte und Bachelor

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

Forschung: MNM Team



MNM
TEAM
MUNICH NETWORK MANAGEMENT TEAM



der Bundeswehr
Universität  *München*