# IT-Sicherheit

## - Sicherheit vernetzter Systeme -

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

Zeit: Montags, 15:15 – 17:45

Ort: Schellingstraße 3,
Hörsaal S003

# Leibniz-Rechenzentrum

# Inhaltsübersicht

1. Einleitung
   - Internet Worm versus Slammer
   - Stuxnet
   - Snowden
2. Grundlagen
   - Ziele der Informationssicherheit
   - Systematische Einordnung von Sicherheitsmaßnahmen
   - Standard ISO/IEC 27001
   - Abgrenzung Security vs. Safety
3. Technische Angriffe
   - Grundlagen der Angriffsanalyse
   - Bedrohungen (Threats), Angriffe (Attacks), Schwächen (Vulnerabilities), z.B.:
     - Denial of Service
     - Malicious Code
     - E-Mail-Security
     - Mobile Code
     - Systemnahe Angriffe
     - Web-/Netzbasierte Angriffe
   - Bewertung von Schwachstellen (CVSS)
4. Social Engineering
   - Faktor Mensch in der IT-Sicherheit
   - SE Penetration Testing
   - Digitale Sorglosigkeit
5. Rechtliche Aspekte
   - Strafgesetzbuch
   - Datenschutz
   - IT-Sicherheitsgesetz
6. Grundlagen der Kryptographie
   - Steganographie
   - Kyptosysteme: Permutationen, Substitutionen
   - Kryptoanalyse
7. Symmetrische Kryptosysteme
   - Data Encryption Standard (DES)
   - Advanced Encryption Standard (AES)
   - Kryptoregulierung

# Inhaltsübersicht (2)

8. Asymmetrische und hybride Kryptosysteme
   - RSA
   - Schlüssellängen und Schlüsselsicherheit
   - Hybride Systeme
   - Digitale Signaturen

9. Kryptographische Hash-Funktionen
   - Konstruktion von Hash-Fkt.
   - Angriffe auf Hash-Fkt.
   - MD5
   - SHA-3 (Keccak)

10. Sicherheitsmechanismen
    - Vertraulichkeit
    - Integrität
    - Identifikation
    - Authentisierung
    - Autorisierung und Zugriffskontrolle

11. 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

12. Schicht 2: WLAN Sicherheit
    - WEP
    - WPA
    - WPA2

# Inhaltsübersicht (3)

13. Schicht 3: Network Layer
    - IP Gefahren und Schwächen
    - IPSec
    - Schlüsselverteilung mit IKE
14. Schicht 4 - Transport Layer
    - TCP / UDP
    - Secure Socket Layer / Transport Layer Security (SSL/TLS)
15. Schicht 7: Secure Shell (ssh)
    - SSH v1 versus SSH v2
    - Protokoll-Architektur
16. Firewalls und Intrusion Detection Systeme
    - Firewall-Klassen
    - Firewall-Architekturen
    - IDS-Arten
17. Anti-Spam Maßnahmen
18. Beispiele aus der Praxis des LRZ
    - Struktur des MWN
    - Virtuelle Firewalls
    - Secomat
    - Nyx

◉ Was ist nicht Gegenstand dieser Vorlesung
- Fortgeschrittene kryptographische Konzepte ⇒ Vorlesung Kryptologie
- Formale Sicherheitsmodelle und Sicherheitsbeweise

# Einordnung der Vorlesung

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

# Termine und Organisation

- Vorlesungstermine und Raum:
  - Montags von 15:15 – 17:45, Raum S003 (Schellingstr. 3)
- Übung; Beginn 28.10.13
  - Dienstags von 12:15 - 13:45 in Raum S003 (Schellingstr. 3)
  - Übungsleitung:
    Stefan Metzger, metzger@lrz.de u. Michael Grabatin, grabatin@lrz.de
- Skript:
  - Kopien der Folien (pdf) zum Dowload
  - http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2015ws/itsec/
- 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 Vereinbarung

# Schein

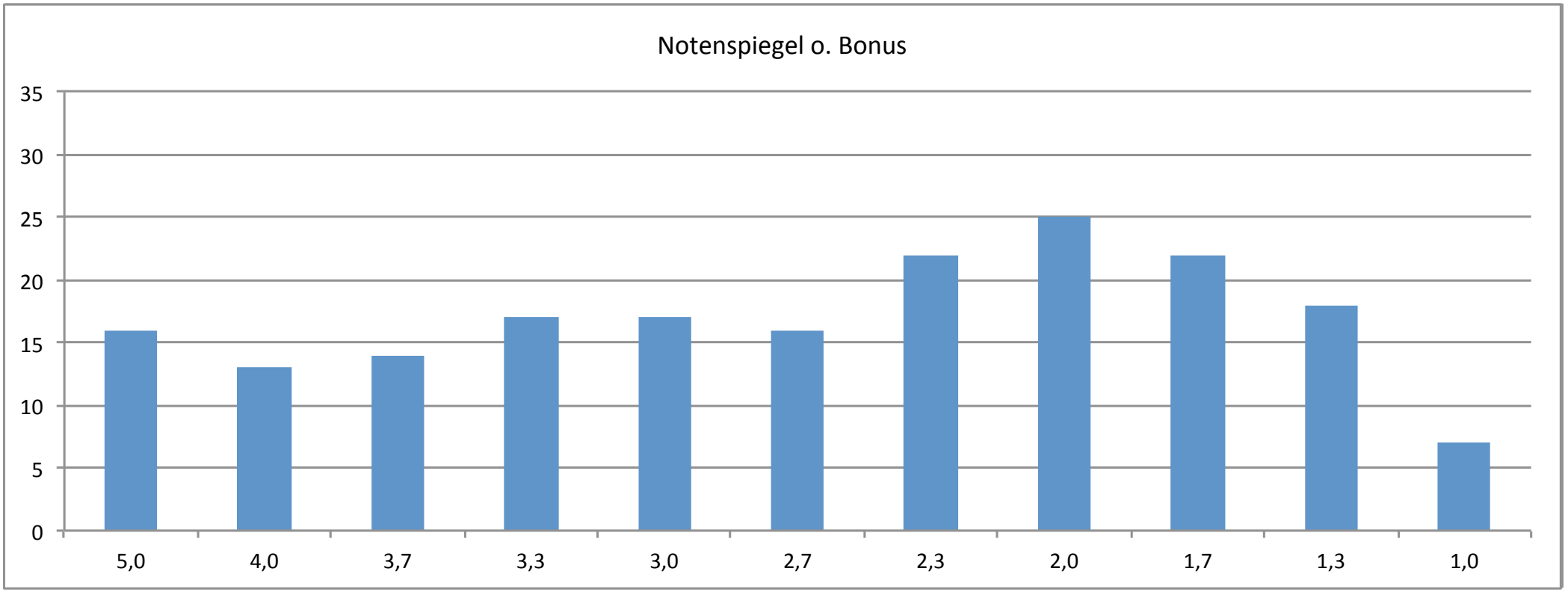
- Anmeldung zur **Übung** und Klausur über uniworx.ifi.lmu.de
- Prüfung zum Erhalt des Scheins
- Notenbonus durch Hausaufgaben
  - Übungsblatt  enthält Hausaufgabe
  - Hausaufgabe bei der Übung abgeben
  - Es werden 4 Blätter / Aufgaben gewählt und korrigiert

| 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

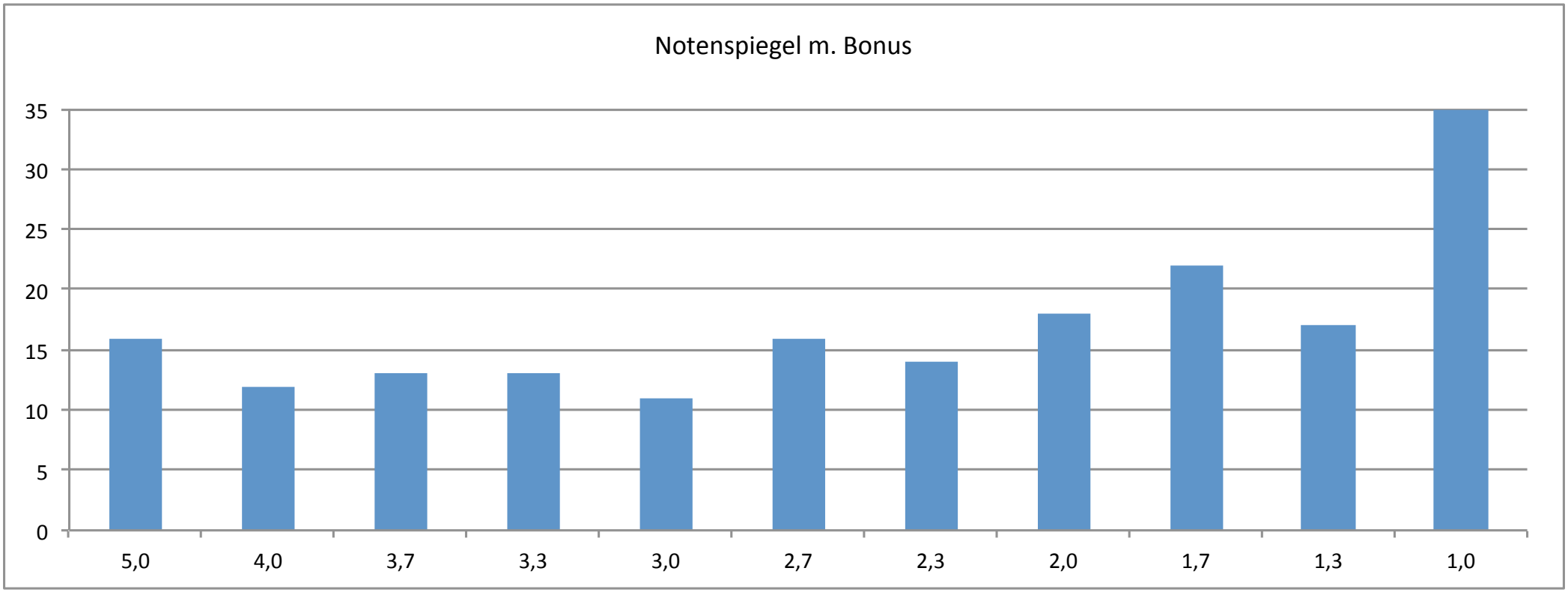
# Notenbonus durch Hausaufgaben: Motivation

- Ergebnisse der letzten Klausur



# Notenbonus durch Hausaufgaben: Motivation

- Ergebnisse der letzten Klausur

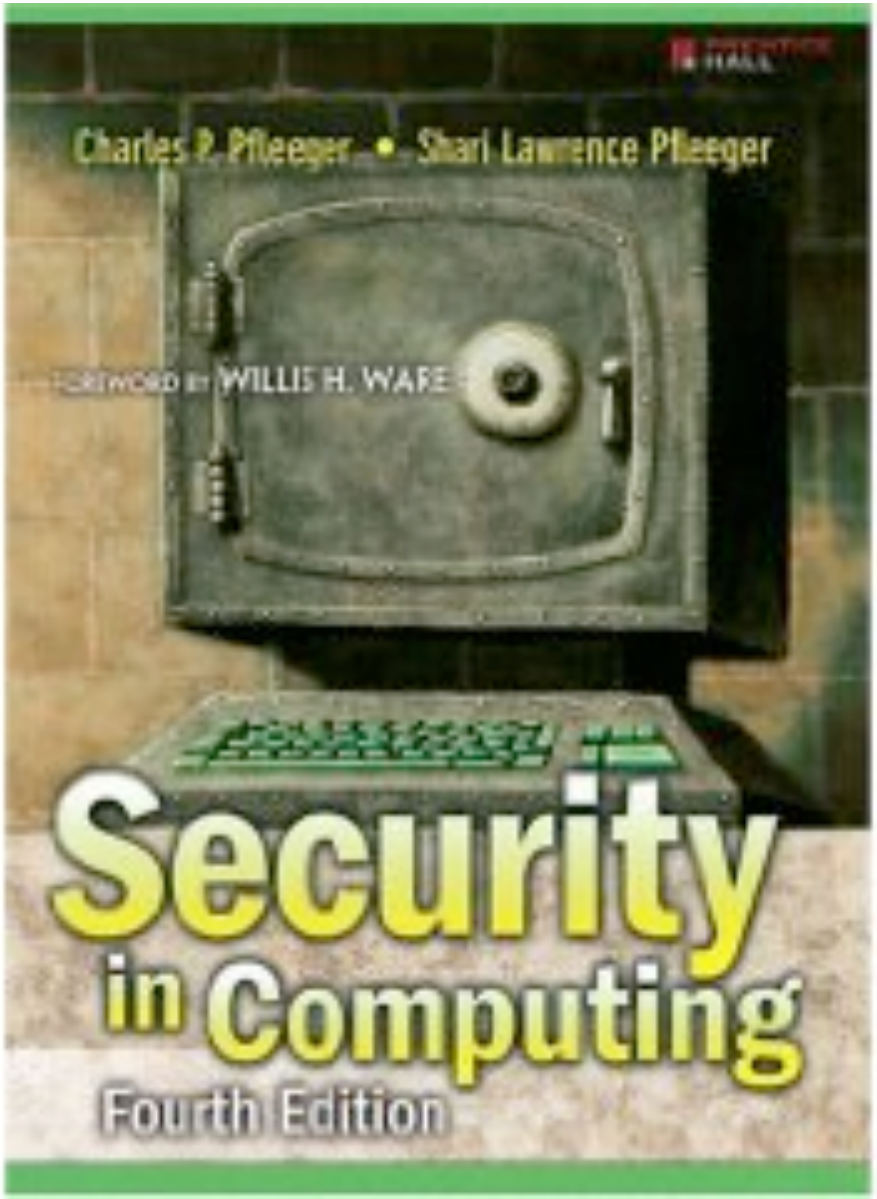


# Literatur: IT-Sicherheit


- Claudia Eckert
  **IT-Sicherheit**
  8. Auflage,
  Oldenbourg-Verlag, 2009
  ISBN 3486578510
  69,80 €

https://opacplus.ub.uni-muenchen.de/search?bvnr=BV040785275

# Literatur: IT-Sicherheit




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

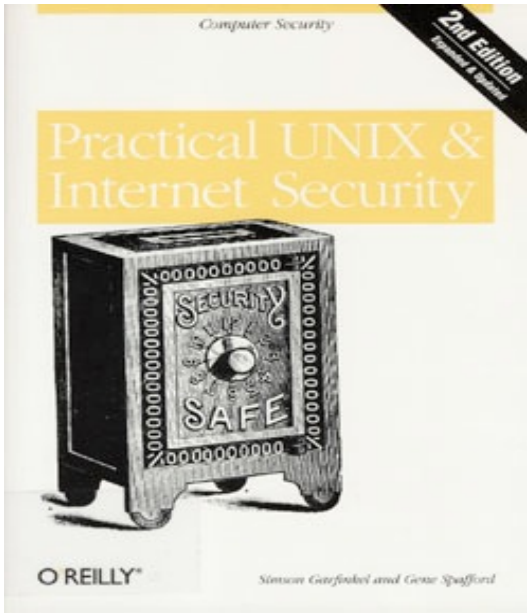
- https://opacplus.ub.uni-muenchen.de/search?bvnr=BV010741294

# Literatur: IT-Sicherheit

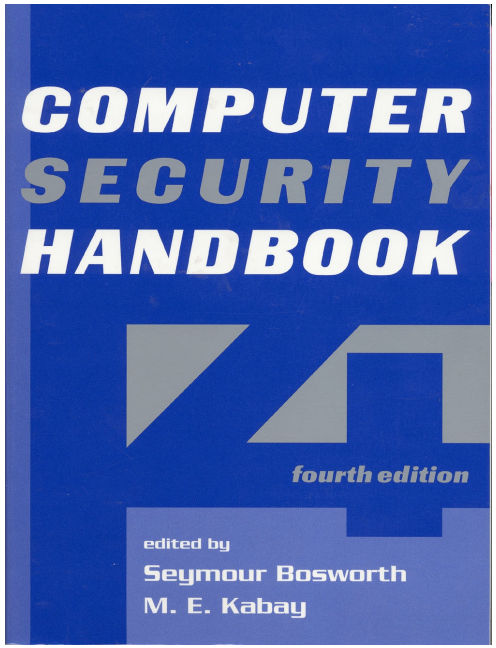

Brenner M., gentschen Felde, N., Hommel, W., Metzger, S., Reiser, H., Schaaf, T.
**Praxisbuch ISO/IEC 27001 - Management der Informationssicherheit und Vorbereitung auf die Zertifizierung**
Hanser, 2011
ISBN-10: 3-446-43026-1
ISBN-13: 978-3-446-43026-6
59,90 €

# Literatur: IT-Sicherheit

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



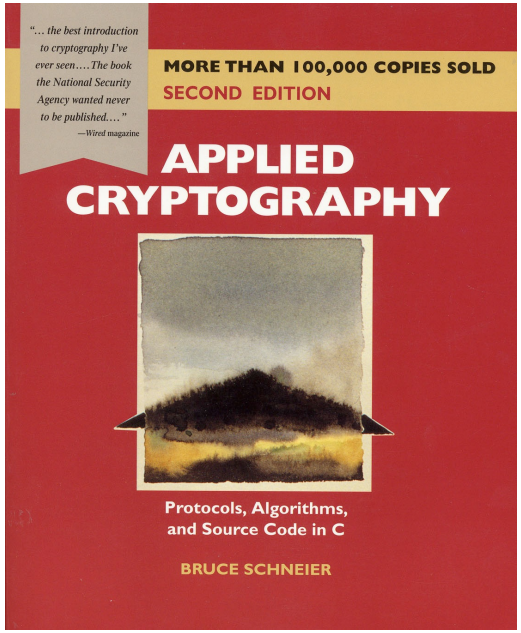

- Seymour Bosworth, M.E. Kabay
  **Computer Security Handbook**
  John Willey & Sons, 2003
  ISBN 0-471-41258-9
  ca. 90 – 100 €

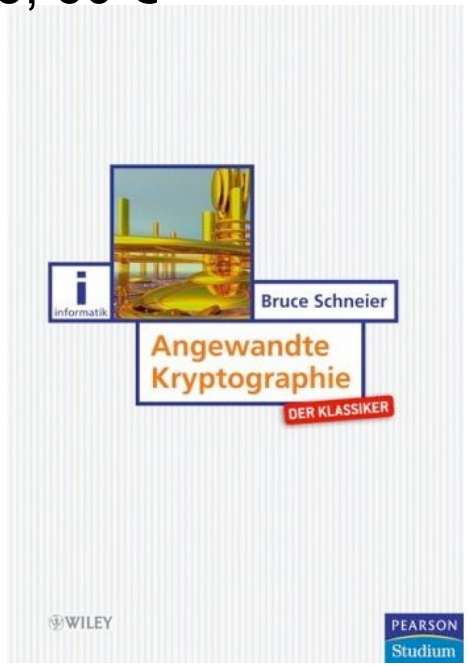



https://opacplus.ub.uni-muenchen.de/search?bvnr=BV014497983

# Literatur: Kryptologie

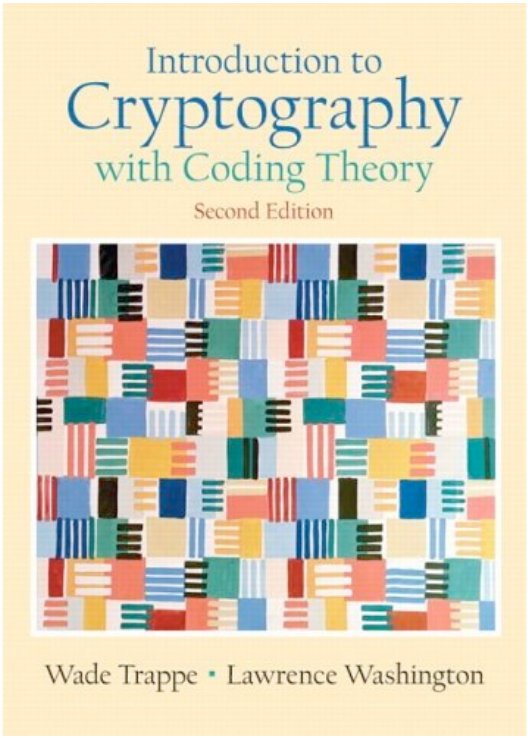
- Bruce Schneier
  **Applied Cryptography**
  John Willey & Sons, 1996
  ISBN 0-471-11709-9
  69 €
  **Angewandte Kryptographie**
  Pearson Studium, 2005
  ISBN 3827372283, 60 €




https://opacplus.ub.uni-muenchen.de/search?bvnr=BV021569735

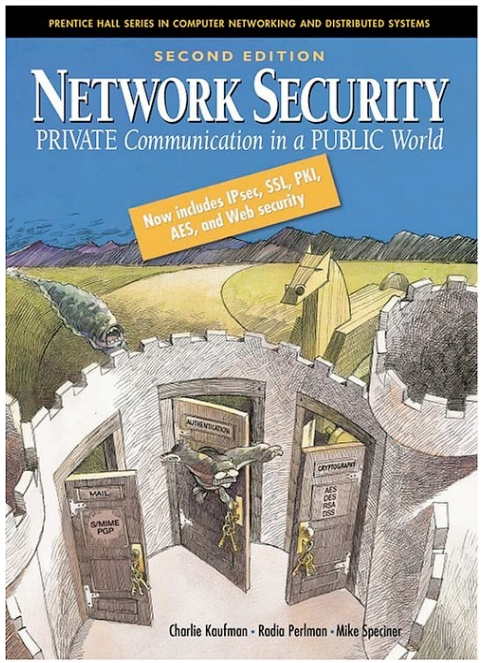
- Wade Trappe, Lawrence C. Washington
  **Introduction to Cryptography with Coding Theory**
  Prentice Hall, 2005
  ISBN 978-0131862395
  83 €



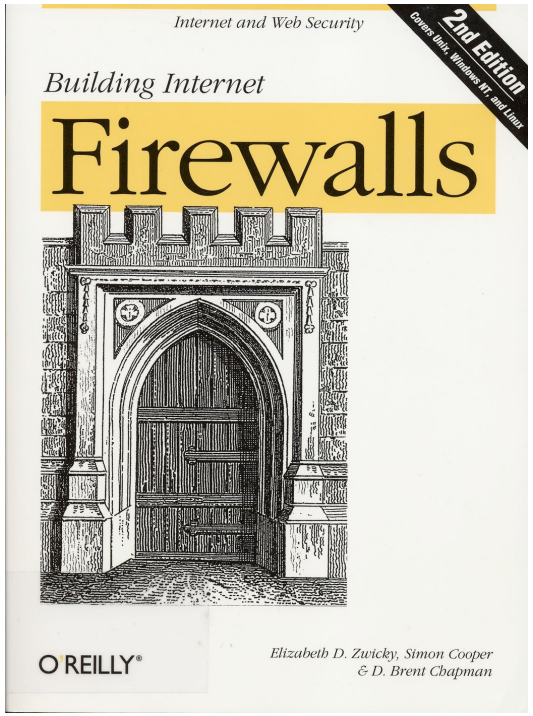

https://opacplus.ub.uni-muenchen.de/search?bvnr=BV014357579

# 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 €




https://opacplus.ub.uni-muenchen.de/search?bvnr=BV036850533

# Weitere Veranstaltungen in diesem Semester

- Vorlesungen:
  - Parallel Computing: Grundlagen und Anwendungen (Prof. Dr. Kranzlmüller, Dr. K. Fürlinger)
    Freitags 9:00 – 12:00, Oettingenstr. 67,
    http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2015ws/parallel/
  - Virtualisierte Systeme (Prof. Dr. Kranzlmüller, PD Dr. Danciu)

# Weitere Veranstaltungen in diesem Semester

- Seminare:
  - Seminar und Praktikum: Wissenschaftliches Arbeiten und Lehren (Prof. Dr. Kranzlmüller, Dr. M. Schiffers)
  - Hauptseminar in Kooperation mit TUM Lst. f. Rechnertechnik und Rechnerorganisation:
    Hochleistungsrechner: Aktuelle Entwicklungen und Trends
    (Prof. Dr. Kranzlmüller, Dr. Führlinger, M.Sc. Maiterth, M.Sc. Fuchs, Prof. Dr. Trinitis (TUM), Dr. Weidendorfer (TUM), Dr. Breitbart (TUM))
  - Kompaktseminar: Prozessorientiertes IT Service Management (Kuhlig (MITSM), Dr. Brenner, Dr. Schaaf, Kemmler, Prof. Kranzlmüller)
  - Masterseminar: Software Defined Networks & Network Function Virtualization (PD Danciu, Prof. Kranzlmüller)

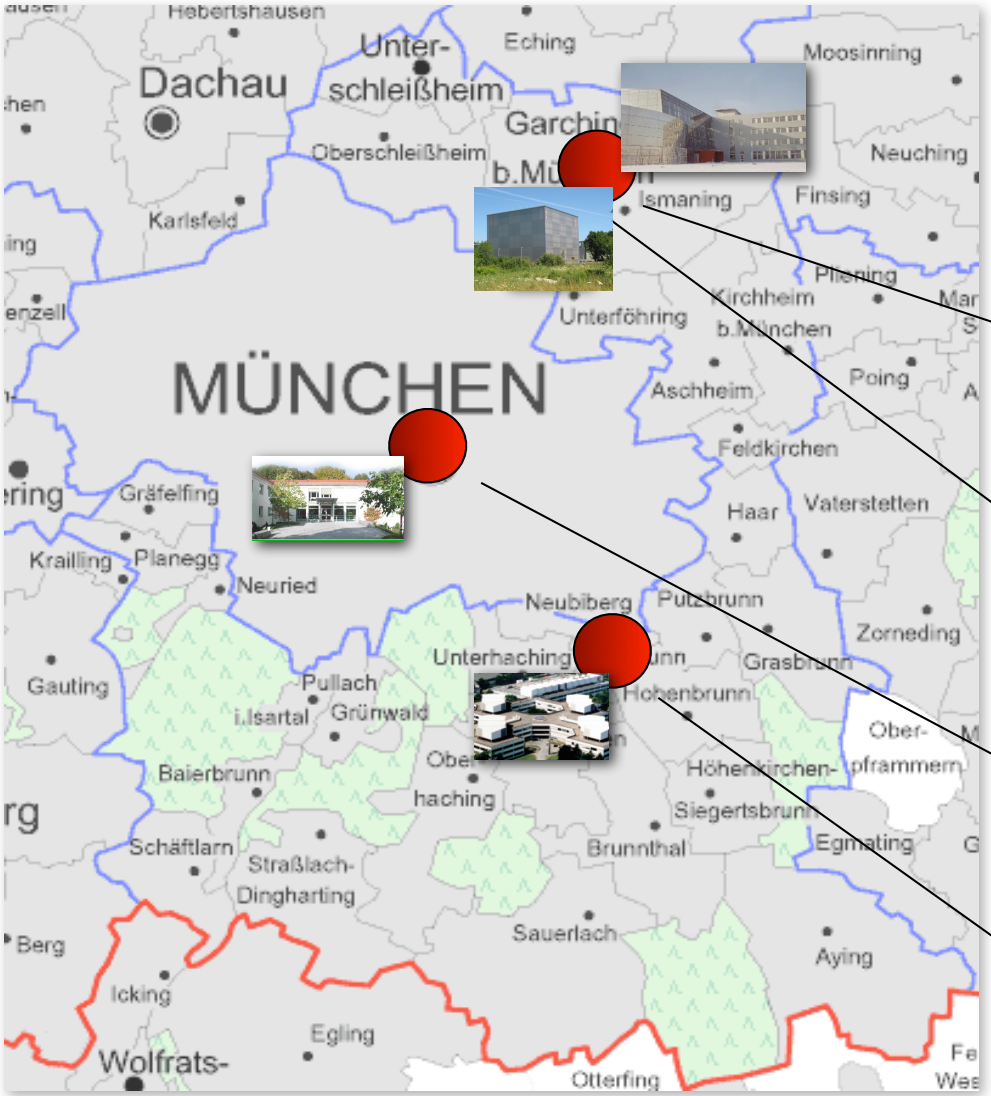
# Weitere Veranstaltungen in diesem Semester

- Praktika:
  - Rechnernetze Praktikum (Prof. Kranzlmüller, Prof. Hegering, PD Danciu, Fuchs)
  - Systempraktikum (Prof. Kranzlmüller, Dr. gentschen Felde, Maiterth)
- Masterarbeiten:

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

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

# Forschung: MNM Team




MNM TEAM
MUNICH NETWORK MANAGEMENT TEAM

der Bundeswehr Universität München