

IT-Sicherheit

- Sicherheit vernetzter Systeme -

The background of the slide is a photograph of a modern, multi-story building with a mix of grey, red, and glass facades. The building is situated on a street with a sidewalk and some trees in the foreground. The sky is blue with some clouds.

Prof. Dr. Helmut Reiser

Zeit: Montags, 14:15 – 16:45

Ort: Schellingstraße 4,
Hörsaal 030



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
 - Kryptosysteme: Permutationen, Substitutionen
 - Kryptoanalyse
7. Symmetrische Kryptosysteme
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Kryptoregulierung

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

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

- **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

■ Vorlesungstermine und Raum:

- Montags von 14:15 – 16:45, Raum 030 (Schellingstr. 4)

■ Übung; Beginn 08.11.16

- Dienstags von 12:15 - 13:45 in Raum S003 (Schellingstr. 3)

- Übungsleitung:

Stefan Metzger, metzger@lrz.de u. Jule Ziegler, ziegler@lrz.de

■ Skript:

- Kopien der Folien (pdf) zum Dowload

- <http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2016ws/itsec/>

■ Kontakt:

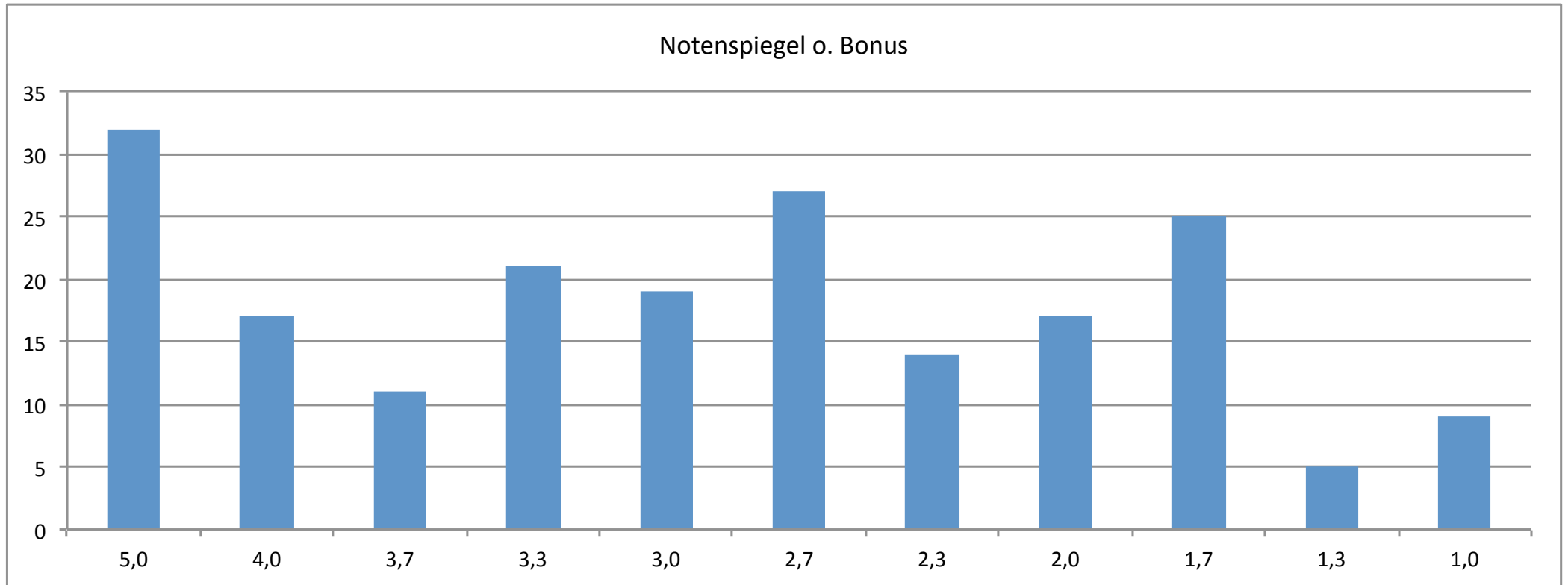
Helmut Reiser
reiser@lrz.de
LRZ, Raum I.2.070

■ Sprechstunde:

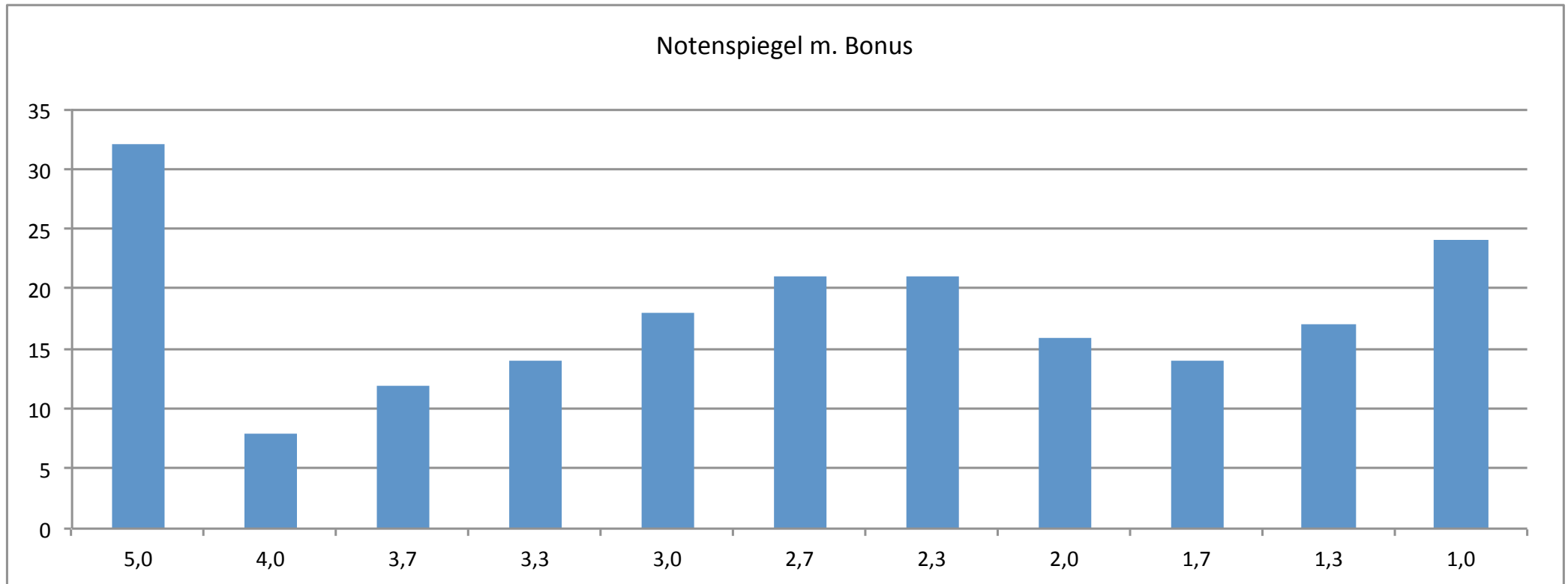
Montags 11:00 bis 12:00 im LRZ; nach der Vorlesung oder nach Vereinbarung

- Anmeldung zur **Übung** und Klausur über uniworx.ifi.lmu.de
- Prüfung zum Erhalt des Scheins
- **Keine Nachholklausur**

■ Ergebnisse der letzten Klausur



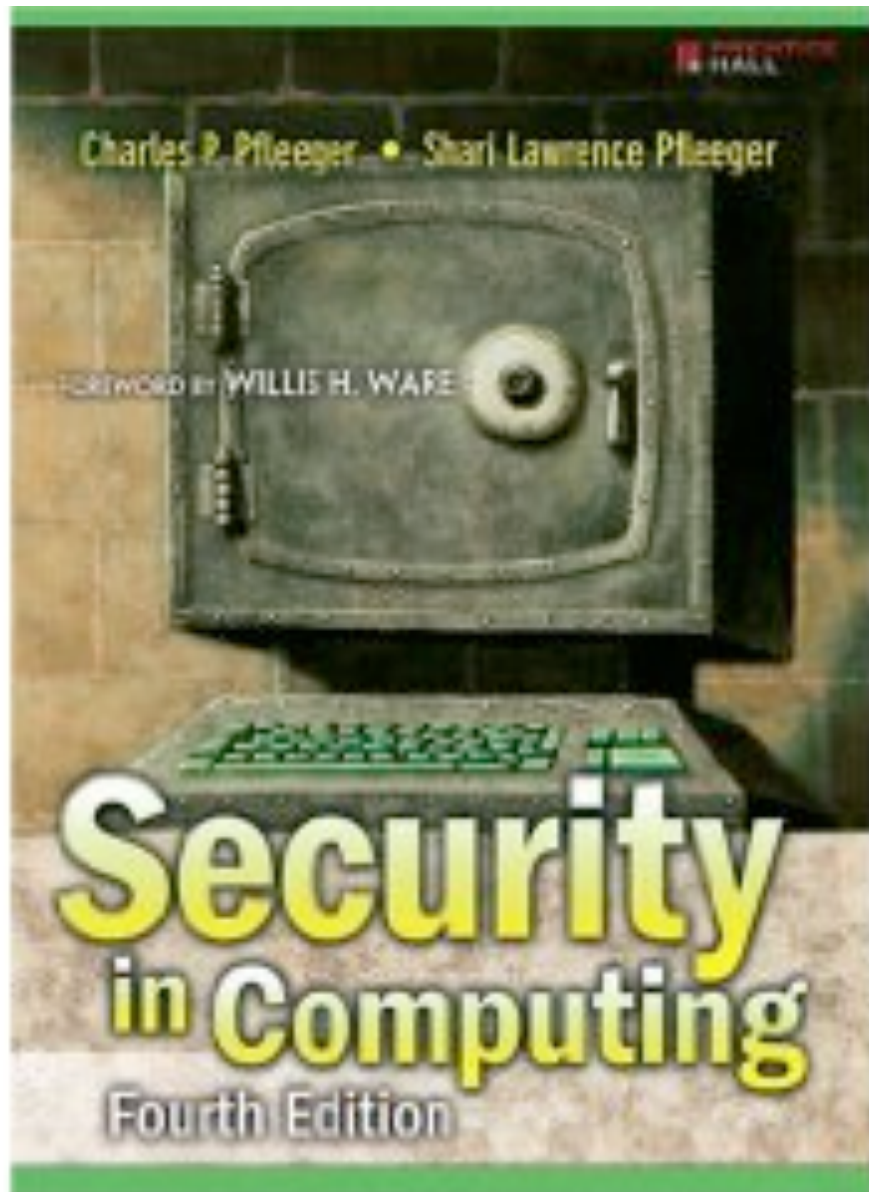
■ Ergebnisse der letzten Klausur





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

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



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

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



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

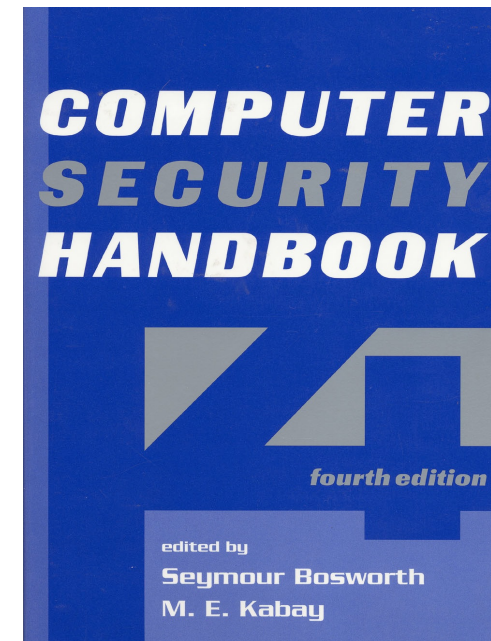
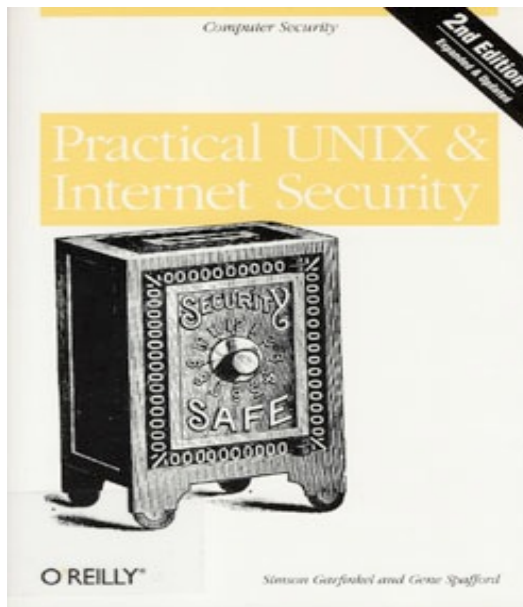
**Praxisbuch ISO/IEC 27001 -
Management der
Informationssicherheit und
Vorbereitung auf die Zertifizierung**
Hanser, 2011

ISBN-10: 3-446-43026-1

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

59,90 €

- Simson Garfinkel, 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>

- Bruce Schneier

Applied Cryptography

John Wiley & Sons, 1996

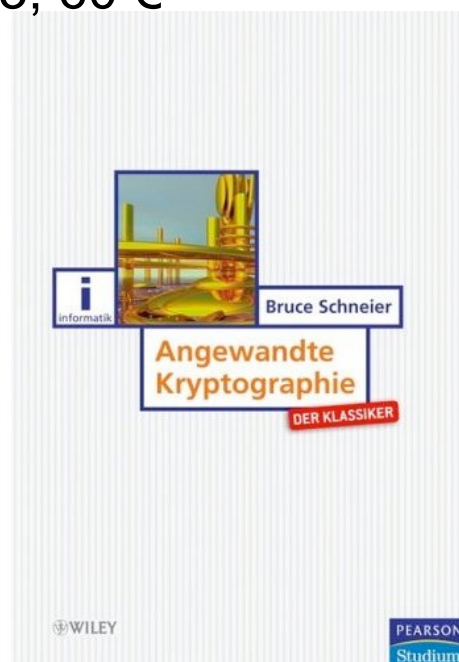
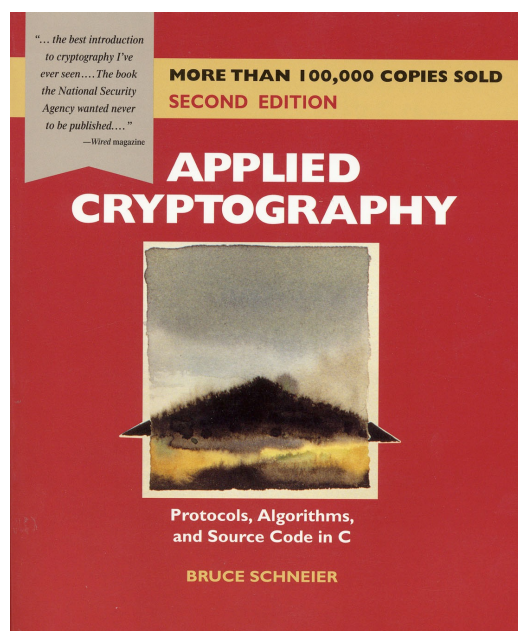
ISBN 0-471-11709-9

69 €

Angewandte Kryptographie

Pearson Studium, 2005

ISBN 3827372283, 60 €



- Wade Trappe, Lawrence C.

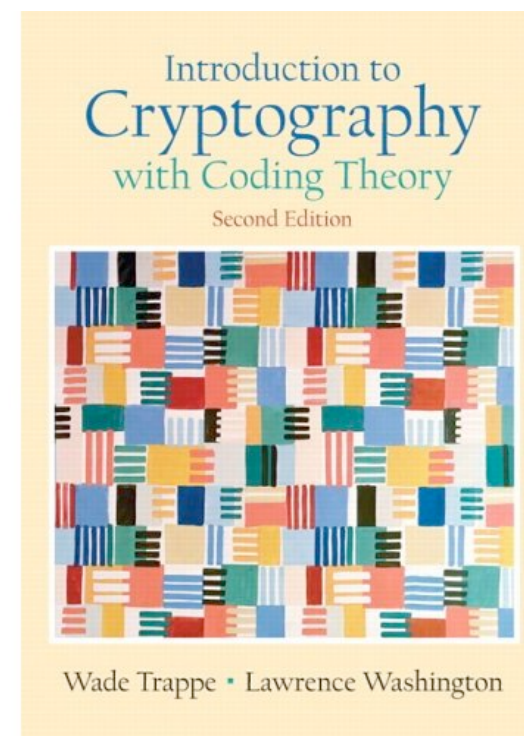
Washington

Introduction to Cryptography with Coding Theory

Prentice Hall, 2005

ISBN 978-0131862395

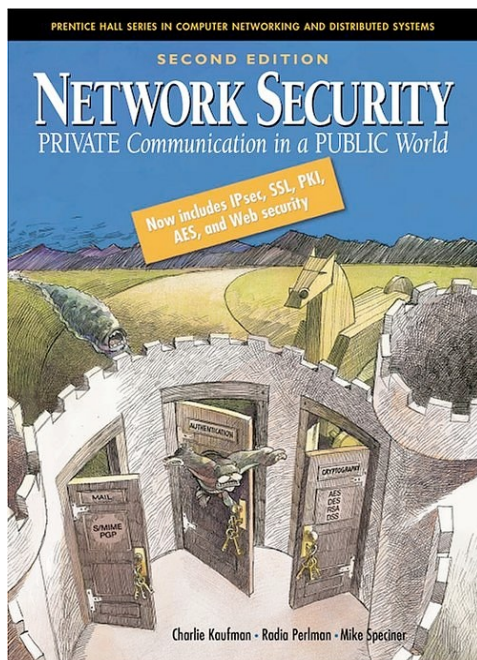
83 €



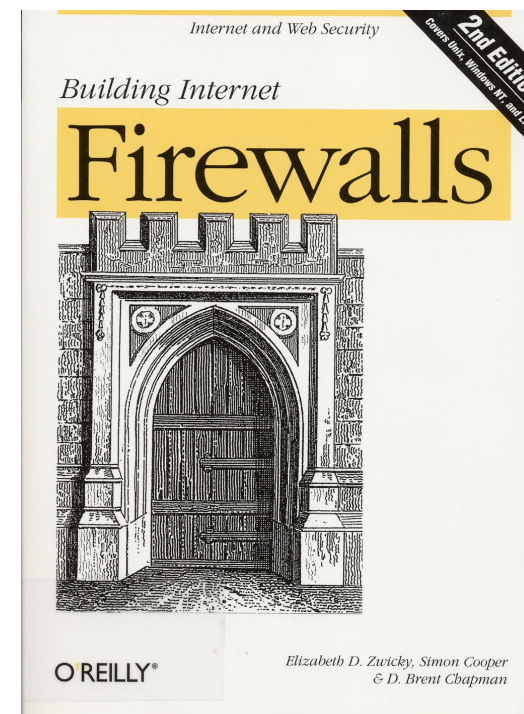
<https://opacplus.ub.uni-muenchen.de/search?bvnr=BV021569735>

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

- 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>

■ Vorlesungen:

- Parallel Computing: Grundlagen und Anwendungen (Prof. Dr. Kranzlmüller, Dr. K. Furlinger, R. Kowalewski)
Freitags 9:00 – 12:00, Oettingenstr. 67, B001
<http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2016ws/parallel/>

■ Seminare:

- Hauptseminar in Kooperation mit TUM Lst. f. Rechnertechnik und Rechnerorganisation:
Hochleistungsrechner: Aktuelle Entwicklungen und Trends
(Prof. Dr. Kranzlmüller, Dr. Führlinger, Prof. Dr. Trinitis (TUM), Dr. Weidendorfer (TUM))
- Hauptseminar und Proseminar: Data Science and Ethics (Prof. Dr. Kranzlmüller, Prof. Dr. Hegering, Dr. gentschen Felde)
- Kompaktseminar: Prozessorientiertes IT Service Management (Kuhlig (MITSM), Dr. Brenner, Dr. Schaaf, Kemmler, Prof. Kranzlmüller)
- Seminar und Praktikum: Wissenschaftliches Arbeiten und Lehren (Prof. Dr. Kranzlmüller, Dr. Schiffers)
- Masterseminar: Software Defined Networks & Network Function Virtualization (PD Danciu, Prof. Kranzlmüller)

■ Praktika:

- Rechnernetze Praktikum (Prof. Dr. Kranzlmüller, T. Guggemos)
- Systempraktikum (Prof. Dr. Kranzlmüller, Dr. gentschen Felde, Maiterth)
- Praktikum Advances Software Development with Modern C++ (Prof. Dr. Kranzlmüller, T. Fuchs)

■ Masterarbeiten:

<http://www.nm.ifi.lmu.de/teaching/Ausschreibungen/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

Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets (14.10.16)

- IoT Devices have been used to create large botnets with self-propagating malware executing DDoS attacks
- Sept. 20, Brian Krebs' security blog was targeted by a 620 Gbps DDoS
 - Mirai Botnet: Scans internet for IoT Devices with 62 default passwords
 - IoT: Home routers, cameras, video recorders
 - 380.000 IoT Devices used for the attack on Krebs' site
 - End of September: DDoS with 1.1 Tbit/s on French web host OVH
- Mitigation:
 - Restart Devices: Mirai exists only in dynamic memory
 - Change password to a secure one
 - Deactivate Universal Plug and Play (UPnP)
 - Update your IoT devices with security patches as soon as available
 - Monitor TCP Port 2323 and 23 (Telnet) and 48101 (used to spread malware)