



IT-Sicherheit

- Sicherheit vernetzter Systeme -



Prof. Dr. Helmut Reiser

Zeit: Montags, 14:15 – 16:45

Ort: Hauptgebäude,
Audimax, A030



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 A030 (Audimax, Hauptgebäude)

■ Übung; Beginn 31.10.17

- 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/2017ws/itsec/>

■ Kontakt:

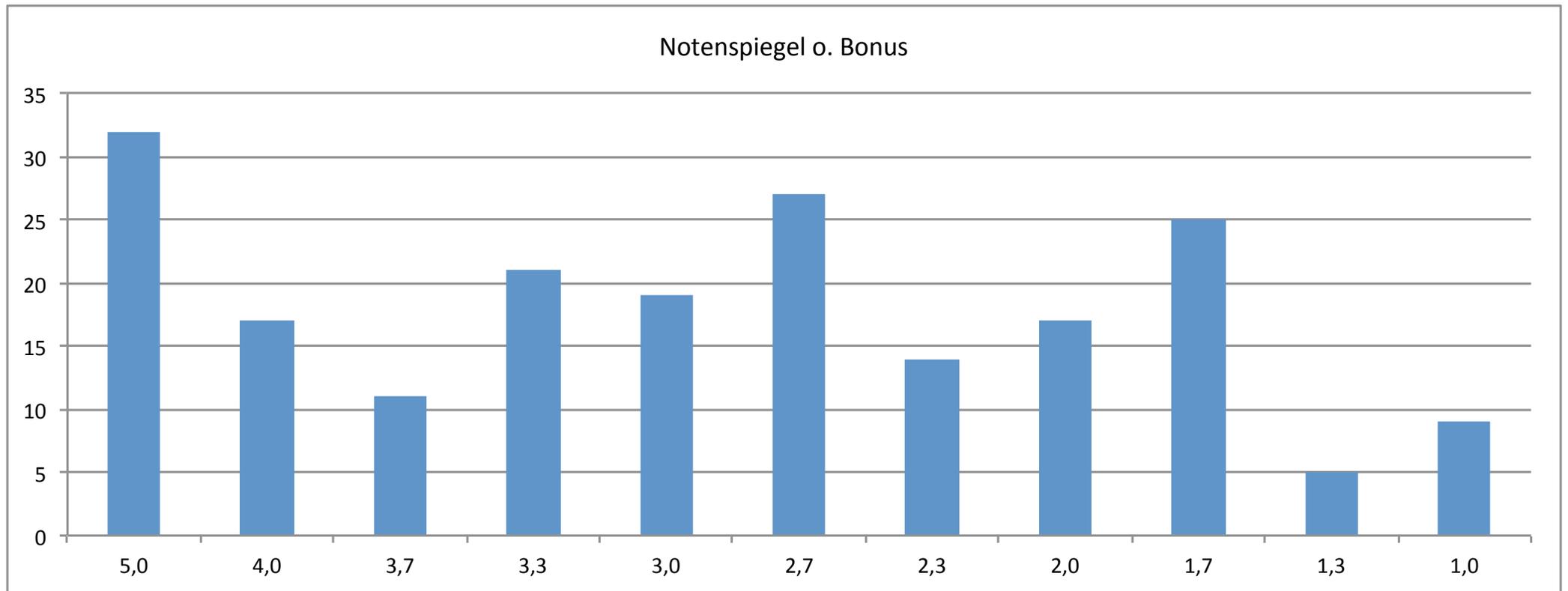
Helmut Reiser
reiser@lrz.de
LRZ, Raum I.3.029

■ Sprechstunde:

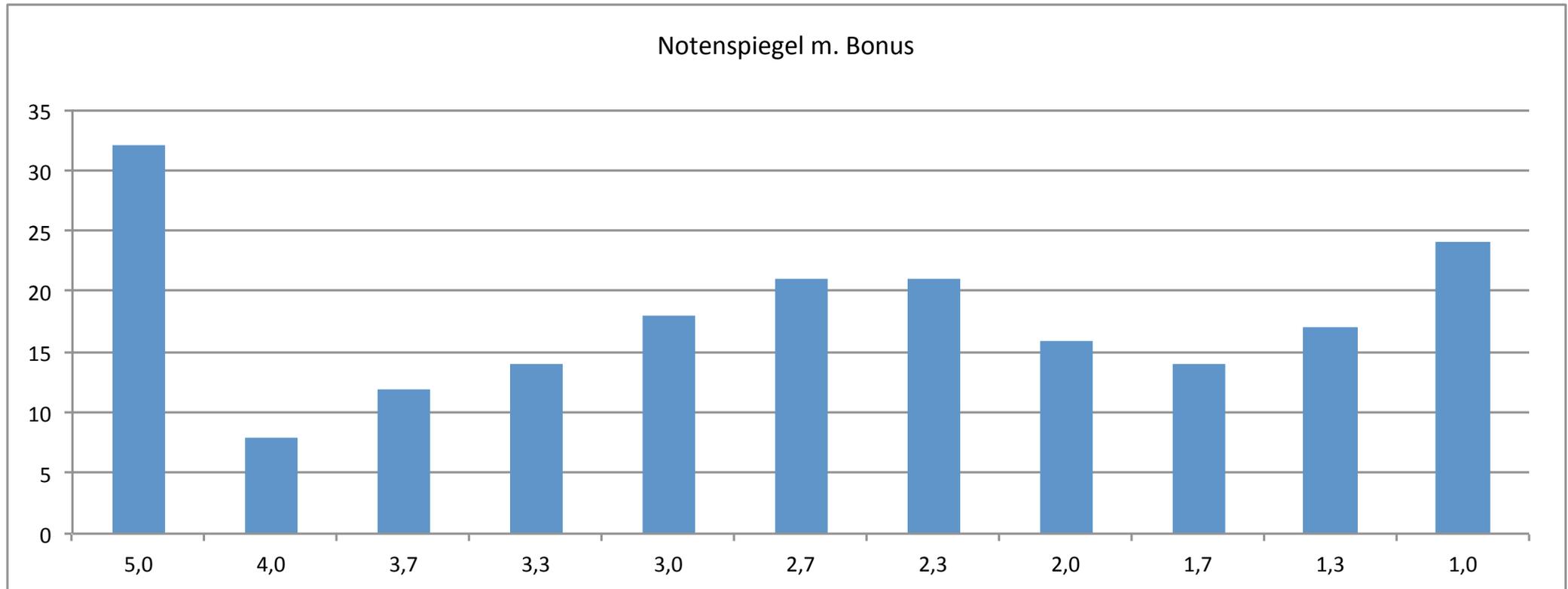
Montags 11:00 bis 12:00 im LRZ; nach der Vorlesung oder nach Vereinbarung

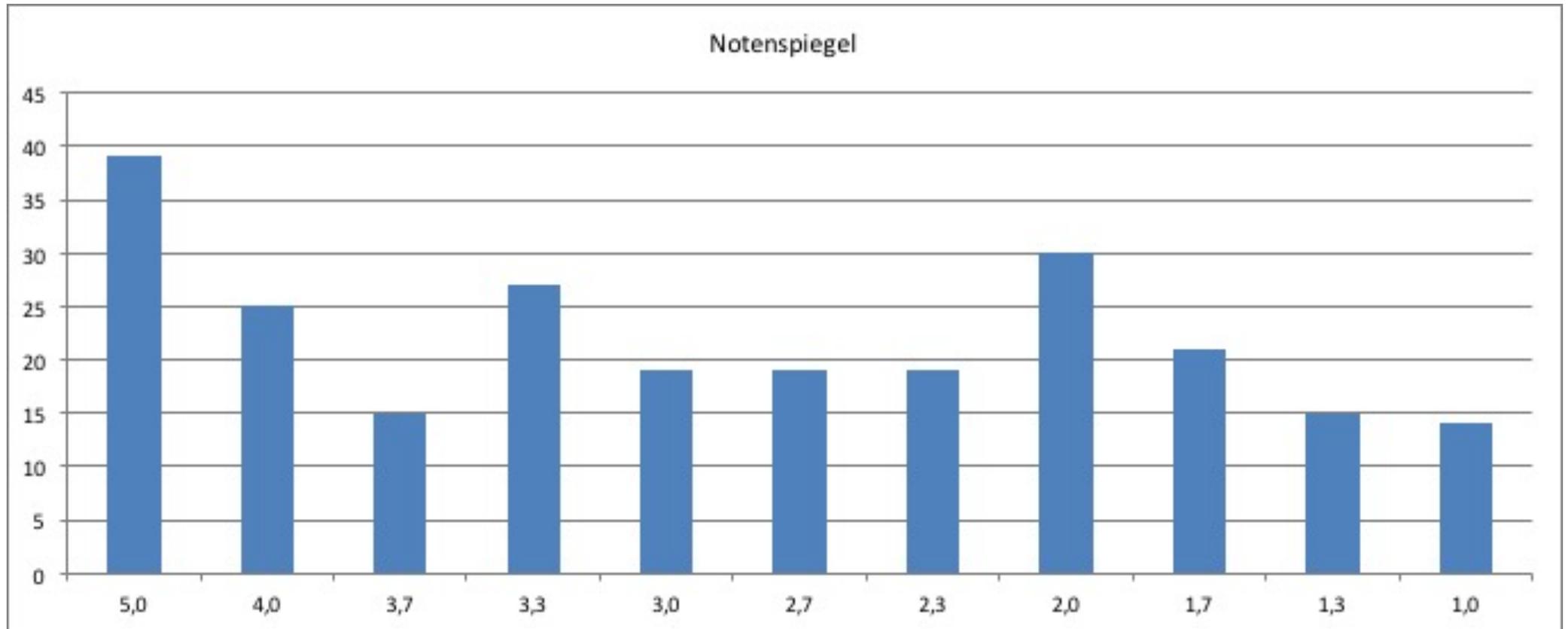
- Anmeldung zur **Übung** und Klausur über uniworx.ifi.lmu.de
- Prüfung zum Erhalt des Scheins
- **Keine Nachholklausur**

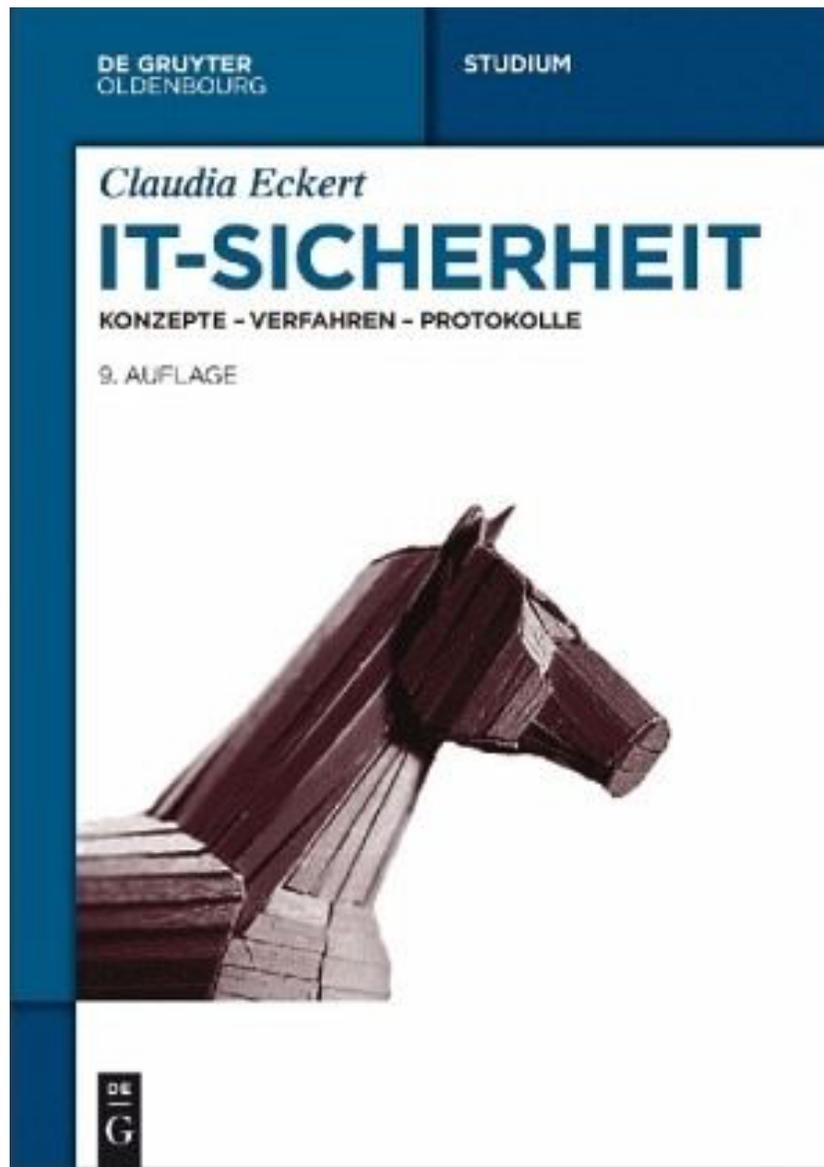
■ Ergebnisse der vorletzten Klausur (WS15/16)



■ Ergebnisse der vorletzten Klausur (WS15/16)

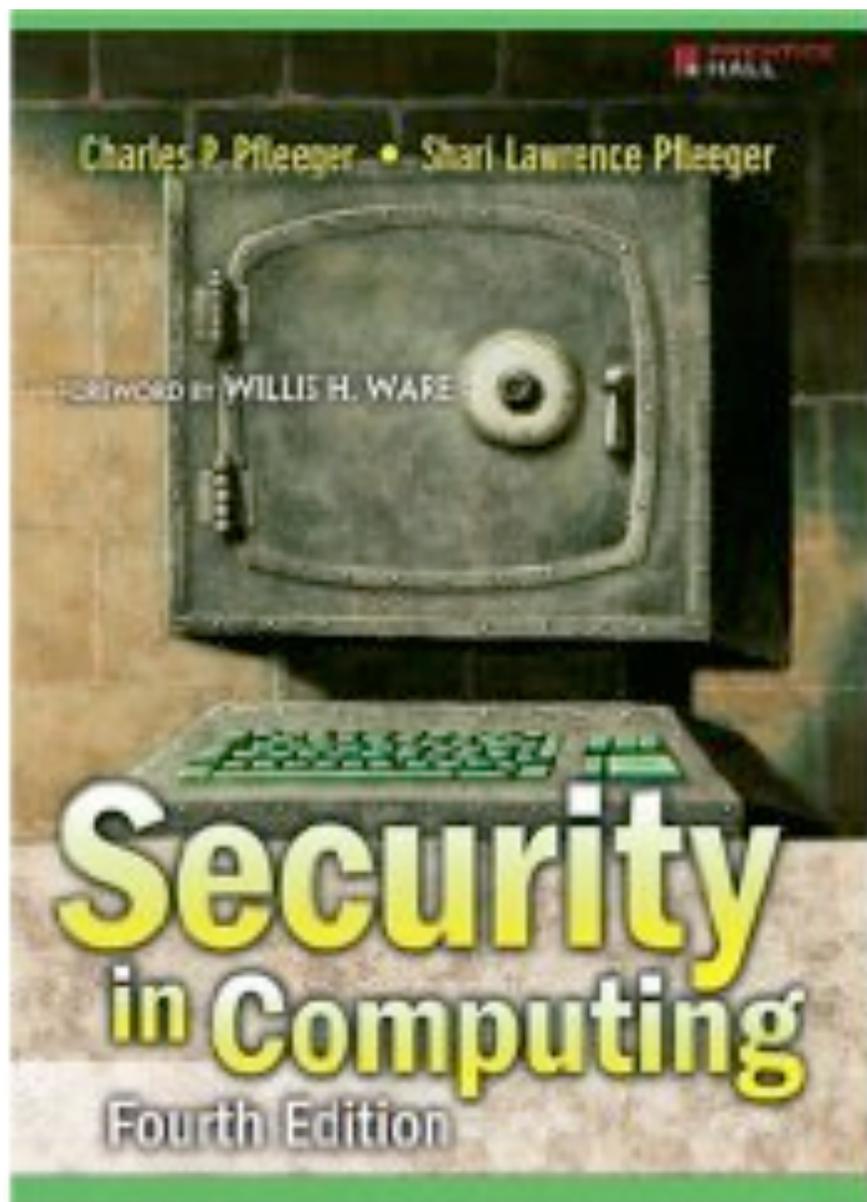






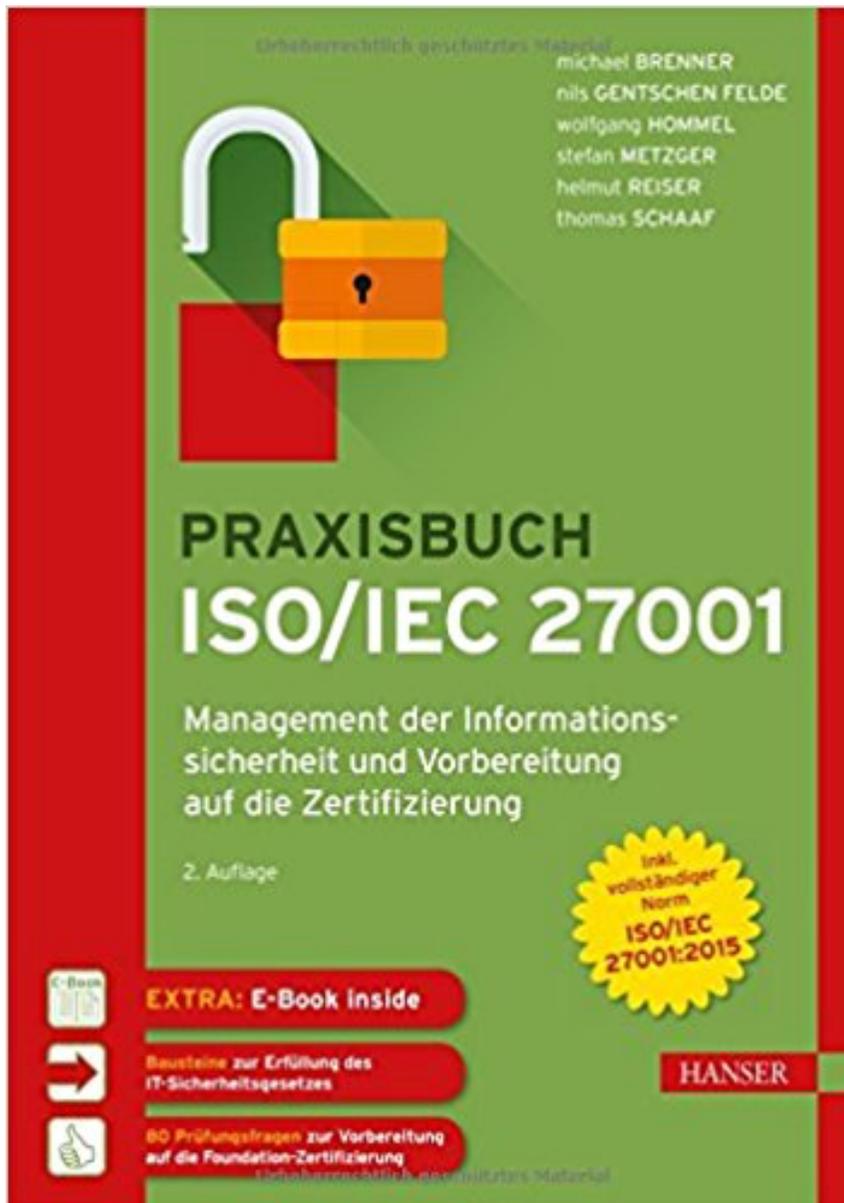
- Claudia Eckert
IT-Sicherheit
9. Auflage,
De Gruyter
69,80 €

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



- 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>

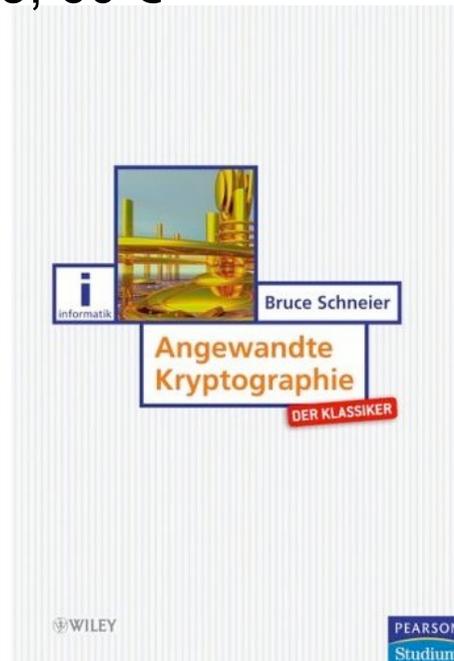
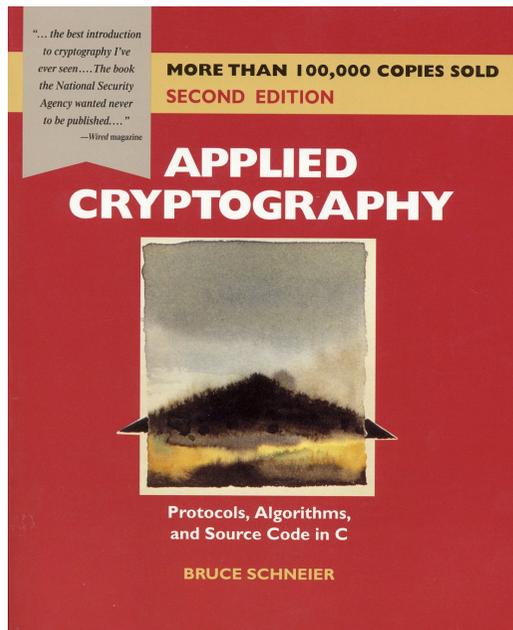


Brenner M., Gentschen Felde, N., Hommel, W., Metzger, S., Reiser, H., Schaaf, T.

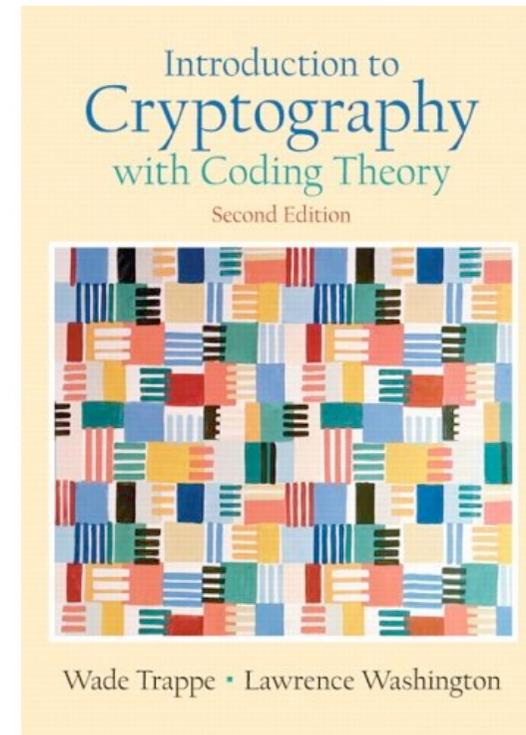
**Praxisbuch ISO/IEC 27001 -
Management der
Informationssicherheit und
Vorbereitung auf die Zertifizierung**
2. Auflage

Hanser, 2017
64 €

- Bruce Schneier
Applied Cryptography
John Wiley & Sons, 20. Auflage
2017
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>

■ Vorlesungen:

- Parallel and High Performance 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/2017ws/parallel/>
- Grid and Cloud Computing (Prof. Dr. Kranzlmüller, Dr. M. Schiffers, Dr. J. Watzl, T. Guggemoos)
Freitags 14:00 - 17:00, Oettingenstr. 67, B U101
- Introduction to Quantum Computing (Prof. Dr. Kranzlmüller, Prof. Dr. Bubak, Dr. K. Rycerz, T. Guggemoos)
Blockkurs 2.10.-10.10.

■ 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: Rechnernetze (Prof. Dr. Kranzlmüller, Prof. Dr. Hegering, Dr. Luckow)
- 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)

■ Praktika:

- Rechnernetze Praktikum (Prof. Dr. Kranzlmüller, Kowalewski)
- Systempraktikum (Prof. Dr. Kranzlmüller, Dr. gentschen Felde, Schmidt)

■ 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

Aktuelles: WLAN WPA2 Schwachstelle

- Angriff wurde am 16.10.17 bekannt
- Schwachstelle in WPA2:
 - KRACK Key Reinstallation Attack
 - Erlaubt Verwendung von „0“ als Sessionkey
 - Damit Abhören des Funkverkehrs möglich
 - WPA2 Schlüssel ist damit aber nicht kompromittierbar
 - Betroffen insbesondere Android ab Version 6 und Linux
 - Angreifer muss sich in der Nähe des AP aufhalten
 - Verschlüsselung in Anwendungsprotokollen schützt weiterhin
- Patch sowohl für APs als auch Clients erforderlich
- SZ vom 17.10.17

Bundesamt verunsichert Online-Nutzer

Wegen einer Sicherheitslücke im Wlan sollen Verbraucher vorerst keine Bankgeschäfte und Einkäufe über drahtlose Internetzugänge tätigen, warnt die deutsche Cyber-Behörde. Experten widersprechen

- Münchner Wissenschaftsnetz (MWN)
 - Knapp 3.600 Access Points werden betrieben
 - 2.800 davon von Alcatel-Lucent (ALU) sind betroffen
 - Rest von HP ist zu alt, implementiert das angreifbare Protokoll 802.11r noch nicht
- Patch von Alcatel-Lucent wird Mittags veröffentlicht
- Notfallwartung ab 14:00 Uhr
 - ALU APs sind Controller-basiert
 - Zentral konfigurierbarer Update möglich
 - Update für alle APs dauert ca. 2 Stunden

Auslastung (MWN) nach SSIDs

