IT-Sicherheit

- Sicherheit vernetzter Systeme -

Prof. Dr. Helmut Reiser

Zeit: Montags, 15 – 18 Uhr

Ort: Hauptgebäude,
Audimax, A030

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“)
  - Nebenfach, soweit in der jeweiligen Prüfungsordnung erlaubt
- 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 15:00 – 17:30, Raum A030 (Audimax, Hauptgebäude)
- Übung; Beginn 29.10.17
  - Dienstags von 12 - 14 Uhr in Raum S002 (Schellingstr. 3)
  - Übungsleitung:

    Stefan Metzger, metzger@lrz.de, Michael Schmidt, michael.schmidt@lrz.de und Tobias Appel, appel@lrz.de
- Skript:
  - Kopien der Folien (pdf) zum Dowload
  - http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2019ws/itsec/
- Kontakt:

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

- Sprechstunde:

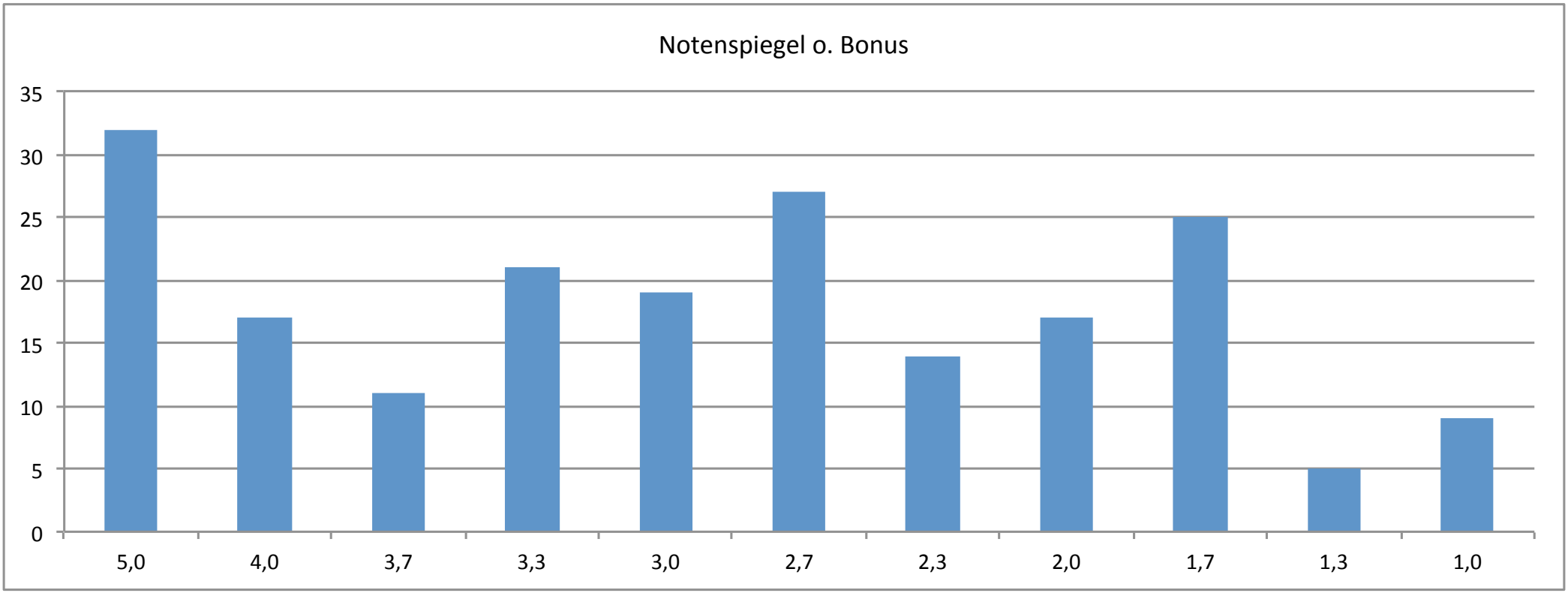
  Montags 11:00 bis 12:00 im LRZ; nach der Vorlesung oder nach Vereinbarung

Schein

- Anmeldung zur Übung und Klausur über uni2work.ifi.lmu.de
- Prüfung zum Erhalt des Scheins
- Keine Nachholklausur

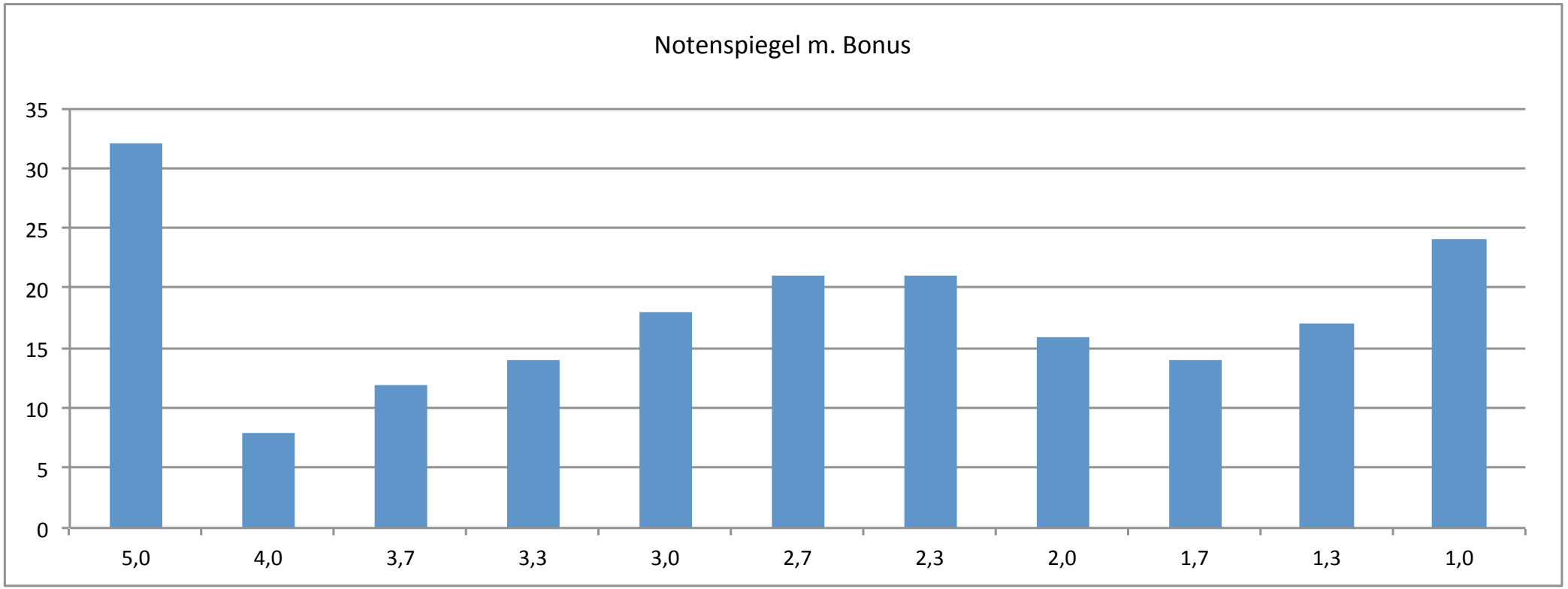
Notenbonus durch Hausaufgaben: Motivation

- Ergebnisse der vorletzten Klausur (WS15/16)

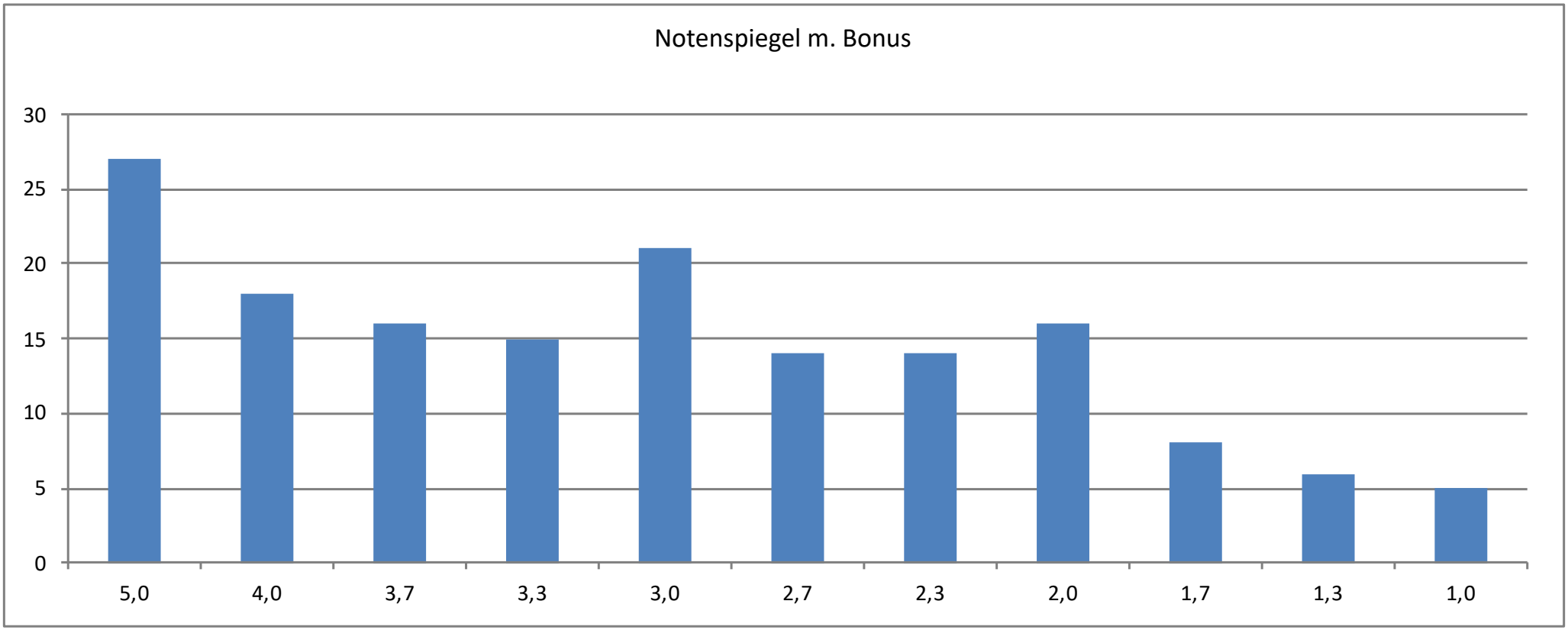


Notenbonus durch Hausaufgaben: Motivation

- Ergebnisse der vorletzten Klausur (WS15/16)



Ergebnisse der letzten Klausur

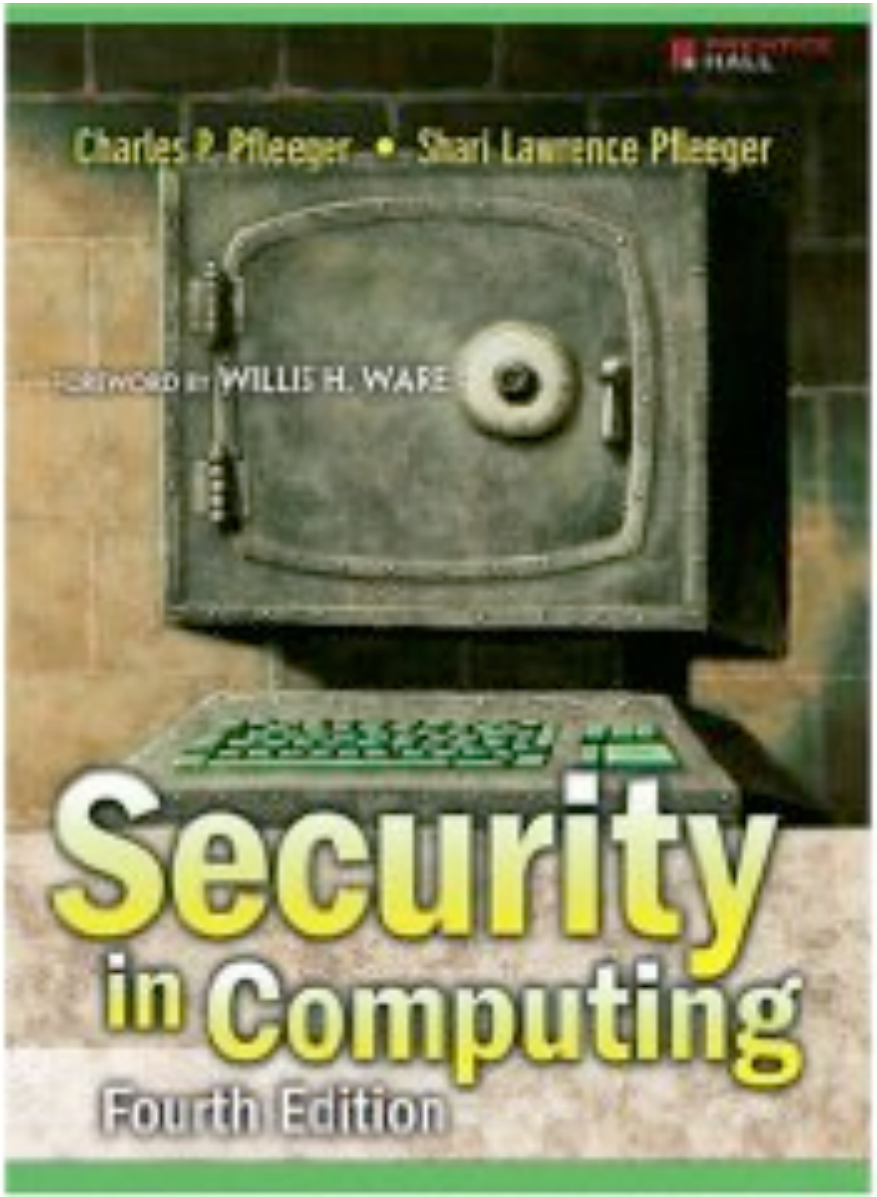


Literatur: IT-Sicherheit

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

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

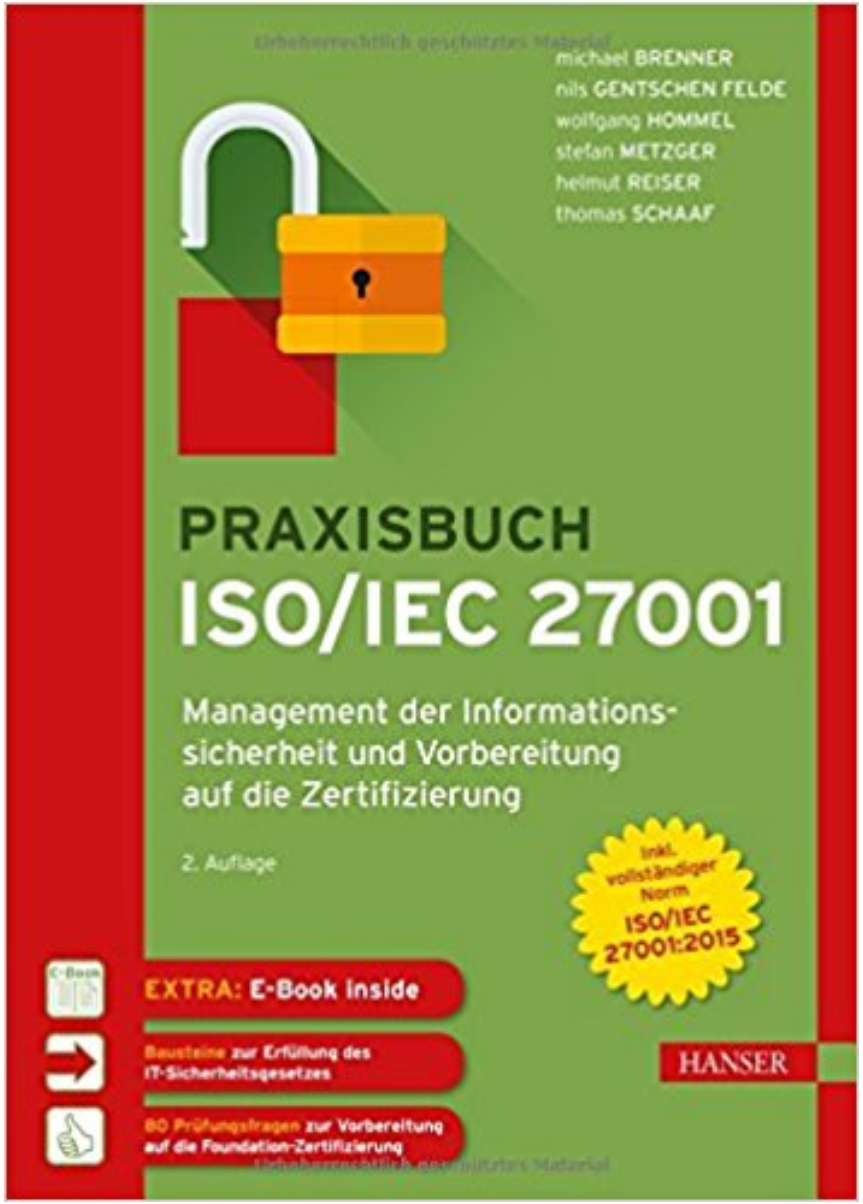
Literatur: IT-Sicherheit



- 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

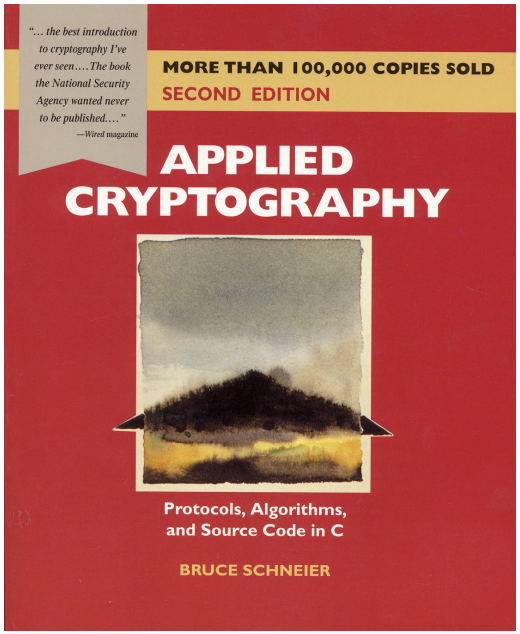


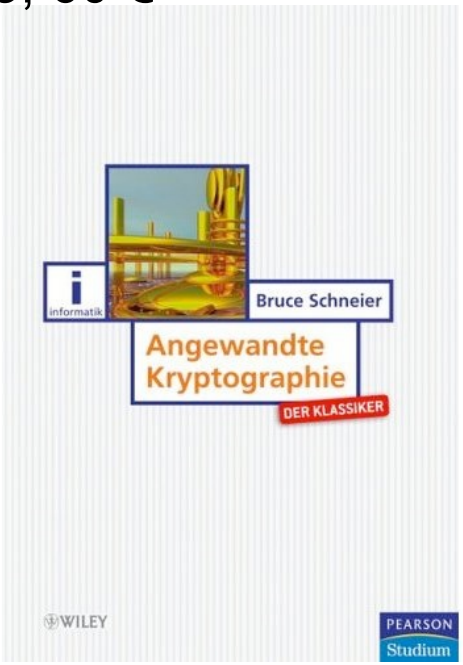
Brenner M., gentschen Felde, N., Hommel, W., Metzger, S., Reiser, H., Schaaf, T.
Praxisbuch ISO/IEC 27001 - Management der Informationssicherheit und Vorbereitung auf die Zertifizierung
2. Auflage

Hanser, 2017
64 €

Literatur: Kryptologie

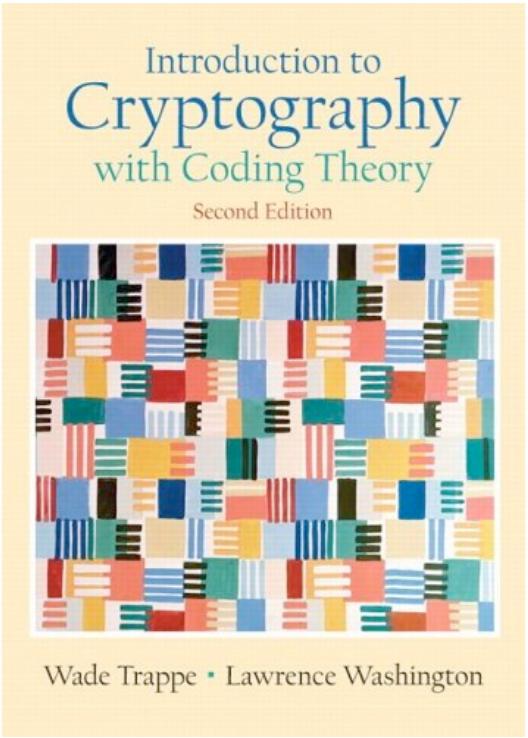
- Bruce Schneier
  Applied Cryptography
  John Willey & Sons, 20. Auflage
  2017
  69 €
  Angewandte Kryptographie
  Pearson Studium, 2005
  ISBN 3827372283, 60 €





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

Weitere Veranstaltungen in diesem Semester

- Vorlesungen:
  - Parallel and High Performance Computing
    (Prof. Dr. Kranzlmüller, Dr. K. Fürlinger)
    Freitags 14:00 – 16:30, Oettingenstr. 67, B U101
    http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2019ws/Parallel/
  - Introduction to Power-Aware HPC (Prof. Dr. Kranzlmüller, Dr. H. Shoukurian)
    Mittwochs 18:15 - 19:45, Oettingenstr. 67, 115
  - Virtualisierte Systeme (Dr. Danciu, Cuong Ngoc Tran)
    Freitags 14:00 bis 16:00 Uhr

Weitere Veranstaltungen in diesem Semester

- Seminare:
  - Hauptseminar:
    Blockchain: Architecture, Algorithms, Infrastructure and Applications
    (Prof. Dr. Kranzlmüller, Dr. Luckow, M. Höb)
  - Proseminar: Blockchain: Architecture, Algorithms, Infrastructure and Applications
    (Prof. Dr. Kranzlmüller, Dr. Luckow, M. Höb)
  - Kompaktseminar: Prozessorientiertes IT Service Management (Kuhlig (MITSM), Dr. Brenner, Dr. Schaaf, Ziegler, Prof. Kranzlmüller)
  - Seminar und Praktikum: Wissenschaftliches Arbeiten und Lehren (Prof. Dr. Kranzlmüller, Dr. Schiffers)

Weitere Veranstaltungen in diesem Semester

- Praktika:
  - Systempraktikum
  - Computer Networks Engineering
  - Virtual Reality

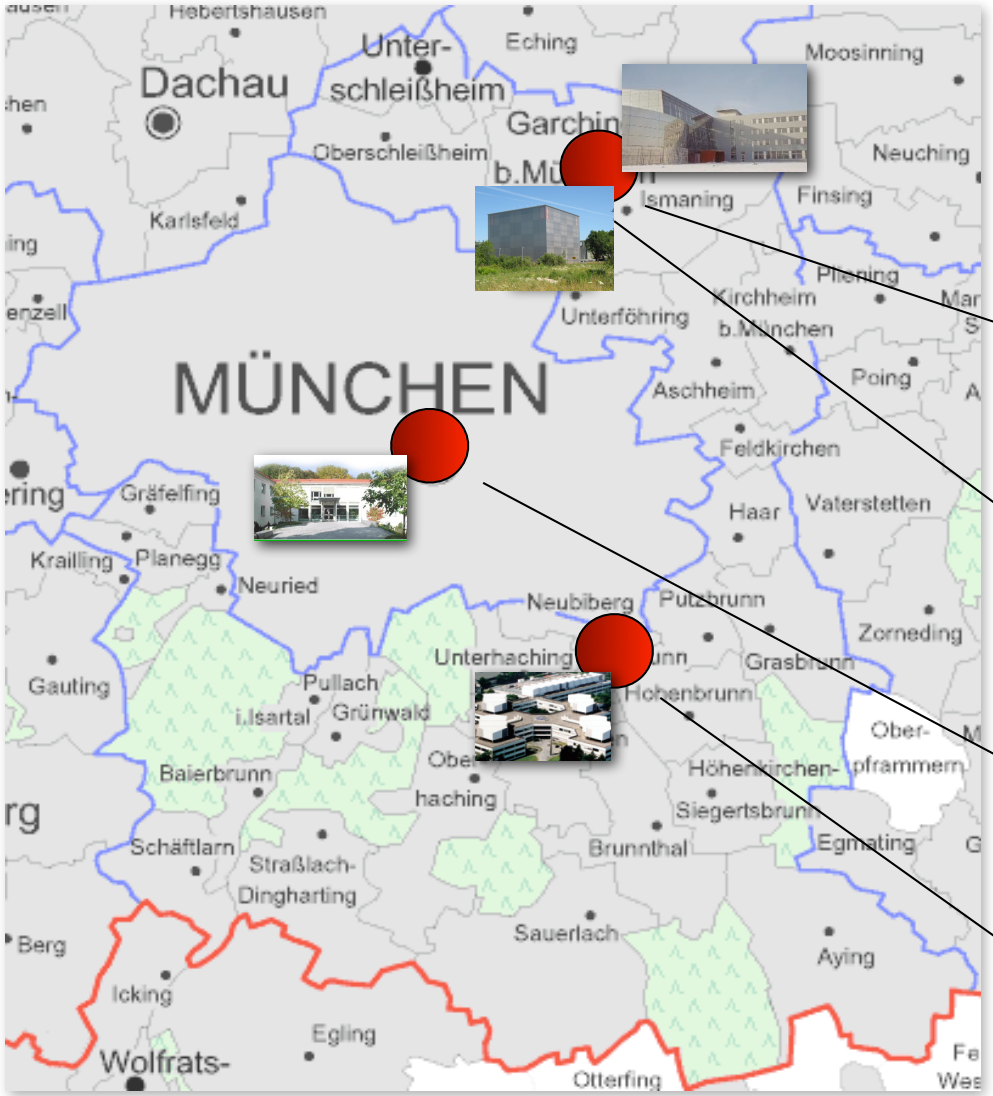
- Masterarbeiten:

  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