IT-Sicherheit

- Sicherheit vernetzter Systeme -

Prof. Dr. Helmut Reiser

Zeit: Montags, 15 – 18 Uhr

Ort: Hauptgebäude,
Audimax, A030

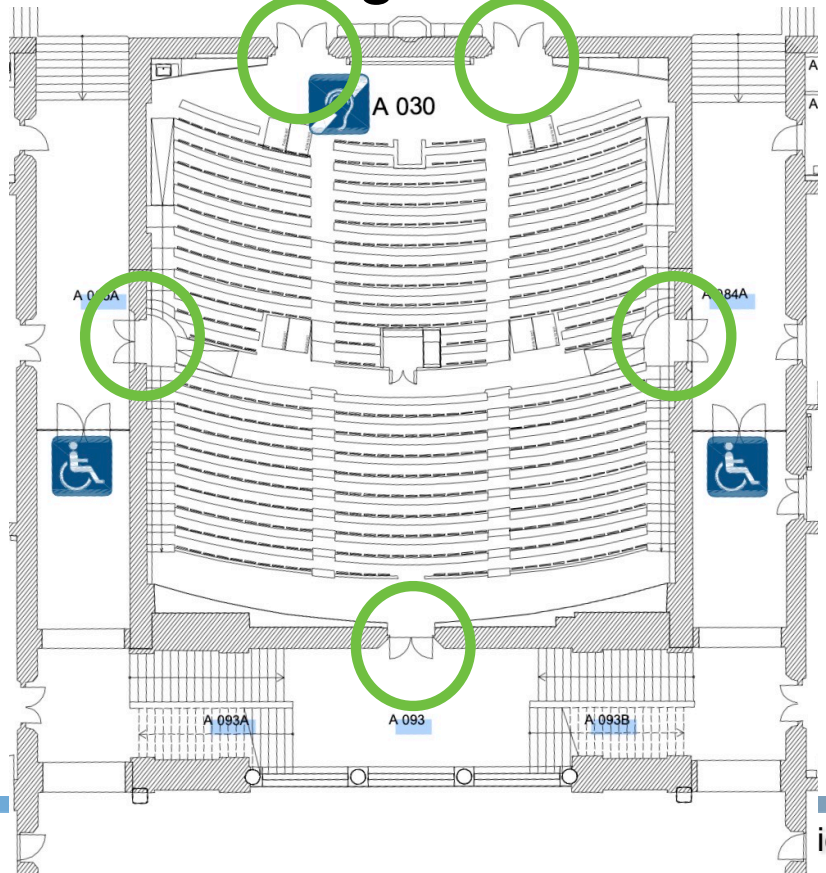
Regeln zum Infektionsschutz (Covid-19)

- Besucher der Vorlesung **sind** zu unterweisen
- Maskenpflicht
  - Inzidenzwert > 35: Maskenpflicht auch im Hörsaal (https://www.muenchen.de/rathaus/Stadtinfos/Coronavirus-Fallzahlen.html)
  - LMU Gebäude insbesondere Verkehrs- und Begegnungsbereiche, Aufzüge, Fluren, Treppenhäuser, Toiletten
- Abstandsgebot einhalten
  - 1,5 m zwischen Personen
  - gilt jederzeit - auch außerhalb der Vorlesung

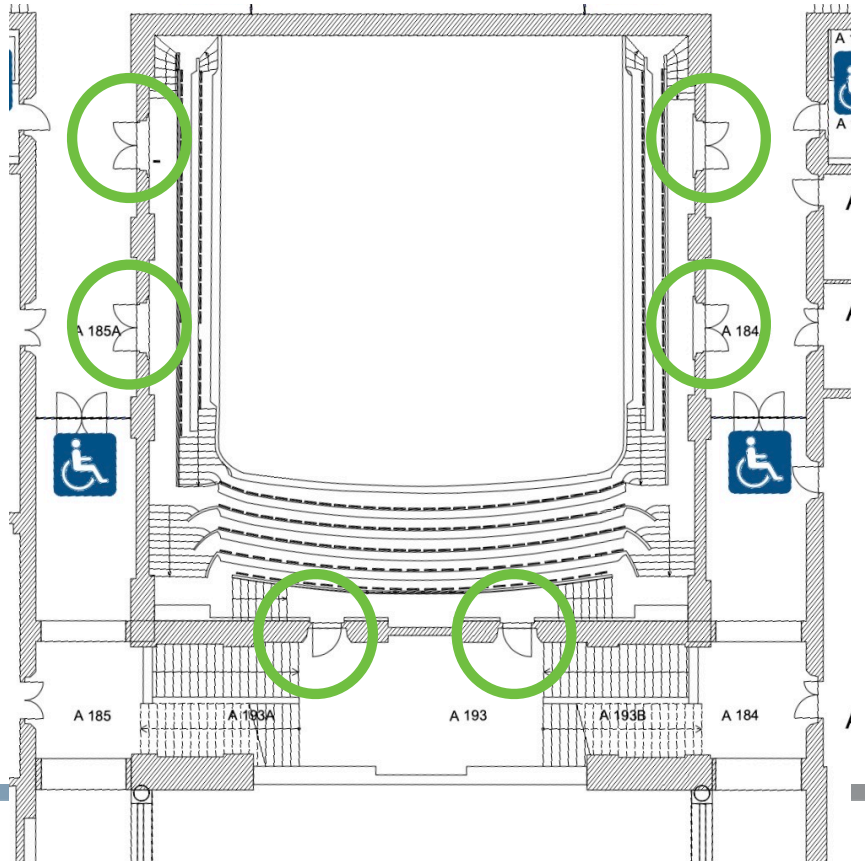
Infektionsschutz: Aufenthalt in der LMU

- Auf notwendige Dauer des Präsenzbetriebes beschränken
- Keine Gruppenbildung
- Mindestabstand jederzeit einhalten
- Beim Betreten des Hörsaals alle Eingänge nutzen

Erdgeschoss



1. OG



Infektionsschutz: Kontaktdatenerfassung

- Jedes Mal QR-Codes an freigegebenen Sitzplätzen scannen
  - Alternativ: https://c.darfichrein.de
- **Beim Verlassen auschecken!!**
- Datenschutz + -sicherheit
  - RZ der Anstalt für kommunale Datenverarbeitung (AKDB)
  - Verschlüsselte Speicherung
  - Löschung nach 1 Monat
  - Zweck: Kontaktdatenerfassung
  - Auf Verlangen an zuständige Gesundheitsämter weiter gegeben
  - Anwesenheitskontrolle ausgeschlossen

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Corona-Platz

BUT-A0.075 Lynen // 292000075_#1

Dieser Platz ist unter Beachtung der Abstandsregeln nutzbar.
Er wird regelmäßig gereinigt.

Zur Nachverfolgung von Infektionsketten sind wir verpflichtet, Ihre Kontaktdaten sowie den Zeitraum Ihrer Anwesenheit zu erfassen.

Für den Schutz Ihrer Daten ist gesorgt. Diese werden verschlüsselt im Rechenzentrum der Anstalt für kommunale Datenverarbeitung in Bayern abgelegt und nur den zuständigen Gesundheitsbehörden auf deren Verlangen hin übermittelt, soweit dies zur Kontaktpersonenermittlung erforderlich ist. Ansonsten werden Ihre Daten nach einem Monat automatisch wieder gelöscht. Eine Anwesenheitskontrolle ist ausgeschlossen.

Weitere Informationen zum Datenschutz finden Sie unter:

www.lmu.de/corona-checkin

So geht's:

BUT-A0.075 Lynen // 292000075 _ #1

1. QR Code mit Handykamera oder QR Code-App scannen.
   (alternativ steht auch ein Scanner unter https://c.darfichrein.de zur Verfügung).
2. Kontaktdaten eingeben, eigenen PIN festlegen und einchecken.
3. Beim Verlassen bitte auschecken.

Sofern Sie kein Smartphone zur Hand haben, melden Sie sich bitte beim Dozenten oder der Dozentin.

DARF ICH REIN.DE

Bayerisches Staatsministerium für Digitales

Darfichrein.de: Die digitale Lösung zur Kontaktdatenerfassung unter der Schirmherrschaft der Bayerischen Digitalministerin Judith Gerlach

Infektionsschutz: Persönliche Maßnahmen

- AHA-Regel: Abstand halten, Hygiene, Alltagsmaske tragen
- regelmäßiges und gründliches Händewaschen mit Wasser und Seife
- kein Händeschütteln oder Umarmen zur Begrüßung
- Korrekter Umgang mit Mund-Nase-Bedeckung
- (Husten und Niesen in die Armbeuge)
- Vermeidung der gemeinsamen Nutzung von Arbeitsmitteln

Infektionsschutz: Verhalten im Verdachtsfall

- Erkrankte Personen oder Verdachtsfälle sind von der Vorlesung ausgeschlossen
  - Kontakt zu Erkrankten in den letzten 14 Tagen (Kontaktpersonen Kategorie I)
  - Gemäß der jeweils gültigen Einreise-Quarantäneverordnung verpflichtet sind, sich 14 Tage in häusliche Quarantäne zu begeben
  - Symptome aufweisen die auf Covid-19 hinweisen könnten:
    - Atemwegssymptome
    - Geruchs- oder Geschmacksstörung
    - Fieber

Infektionsschutz: Risikogruppen

- Angehörigen von Risikogruppen (gemäß RKI)
  - https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Steckbrief.html#doc13776792bodyText15
  - Notwendige Maßnahmen zum Eigenschutz
  - Maßnahmen mit dem Arzt abstimmen

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
- 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 10.11.20
  - Dienstags von 12 - 14 Uhr als Online Veranstaltung
  - 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/2020ws/itsec/
- Kontakt:

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

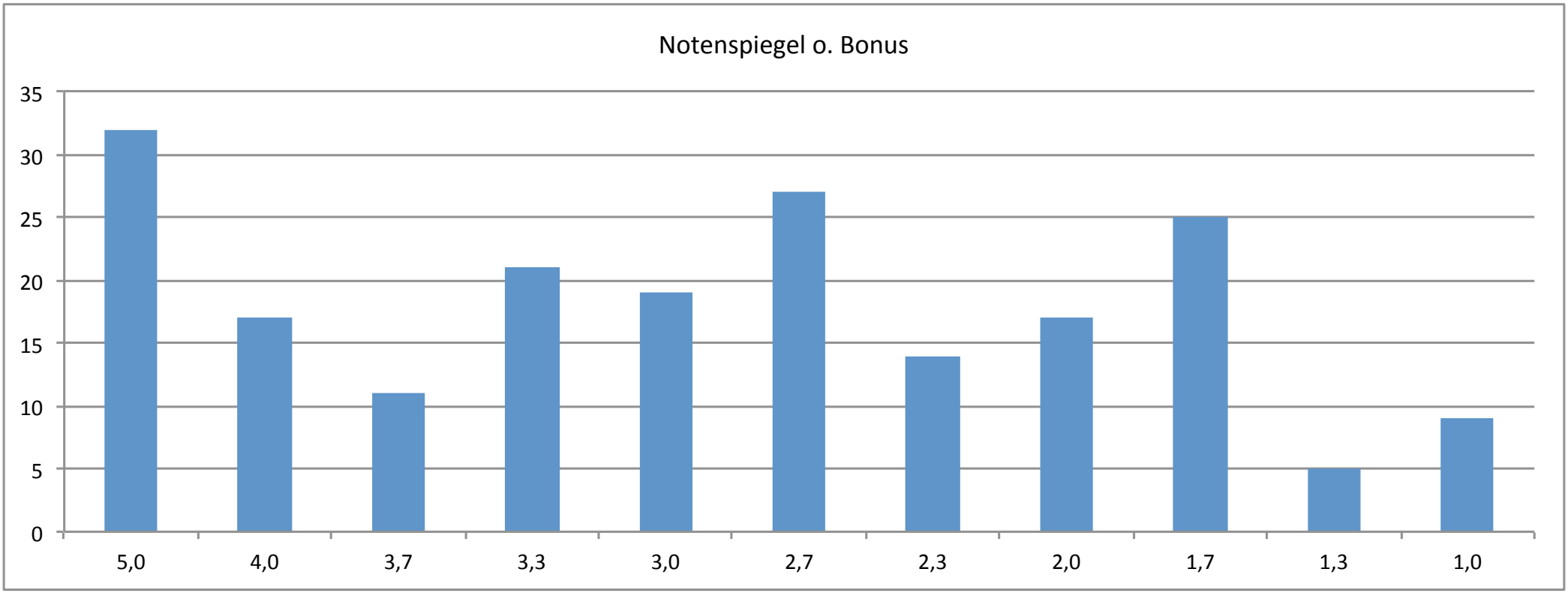
- Sprechstunde:
  nach der Vorlesung oder nach Vereinbarung im LRZ

Schein

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

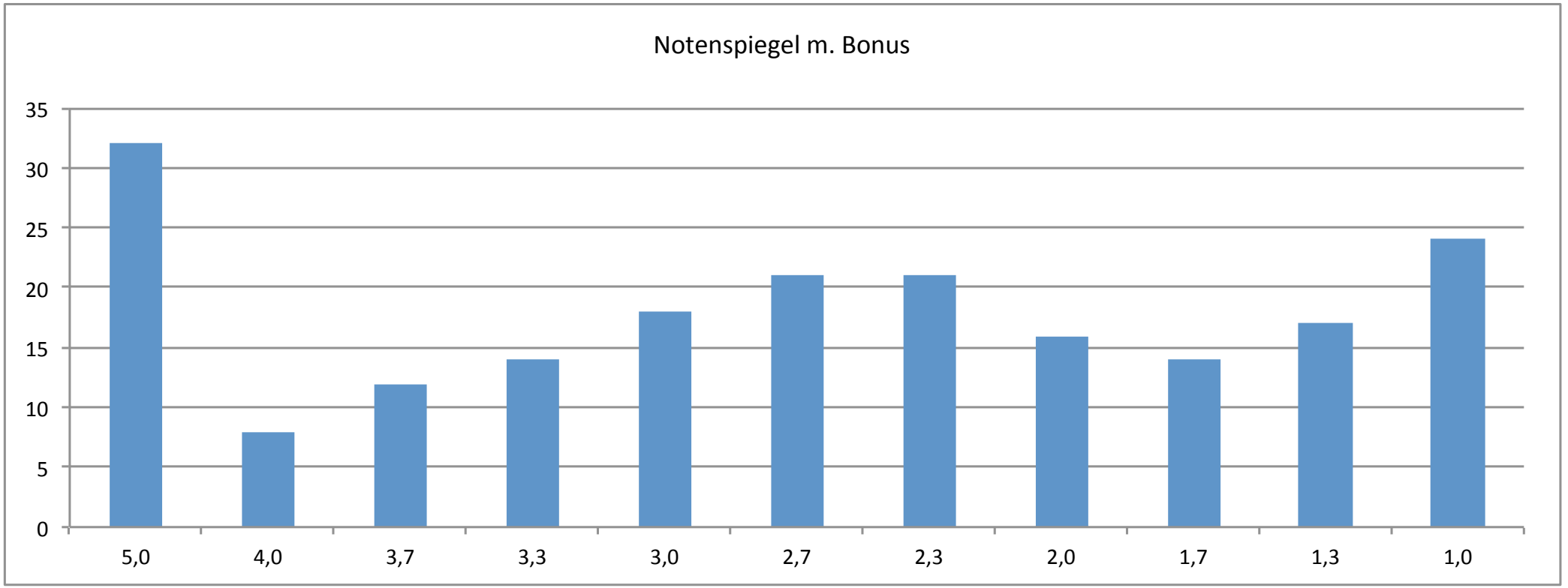
Notenbonus durch Hausaufgaben: Motivation

- Ergebnisse der Klausur WS15/16

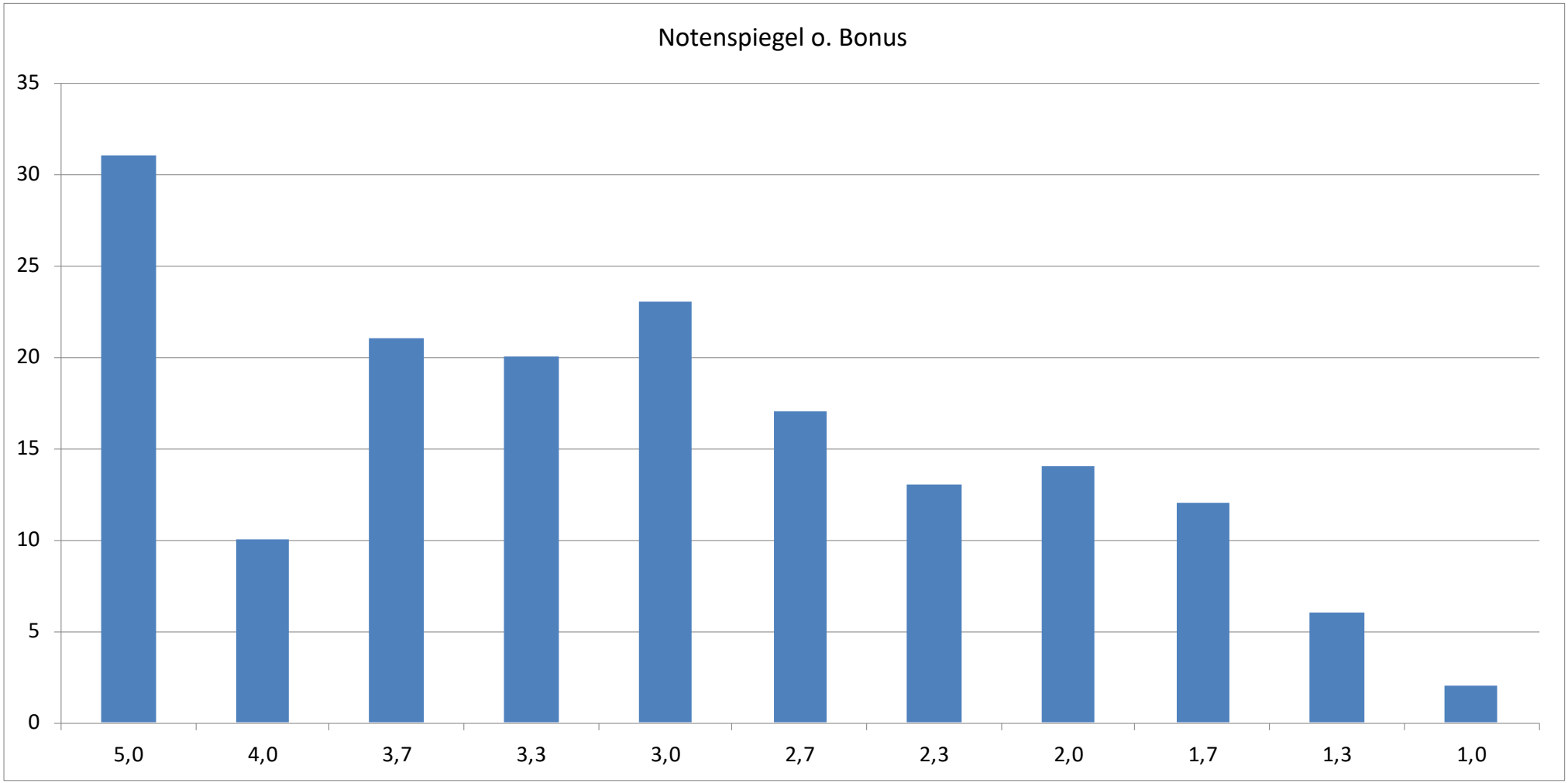


Notenbonus durch Hausaufgaben: Motivation

- Ergebnisse der Klausur WS15/16



Ergebnisse der letzten Klausur

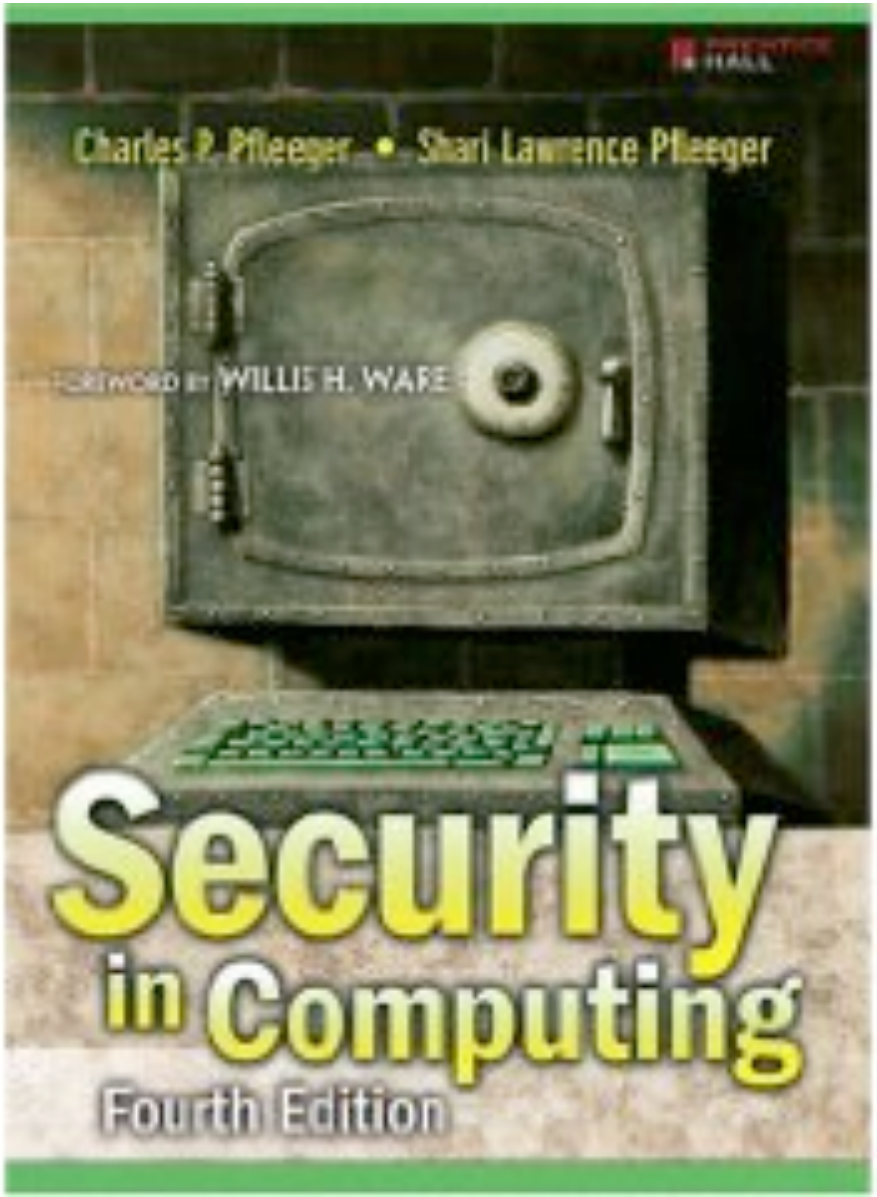


Literatur: IT-Sicherheit

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

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

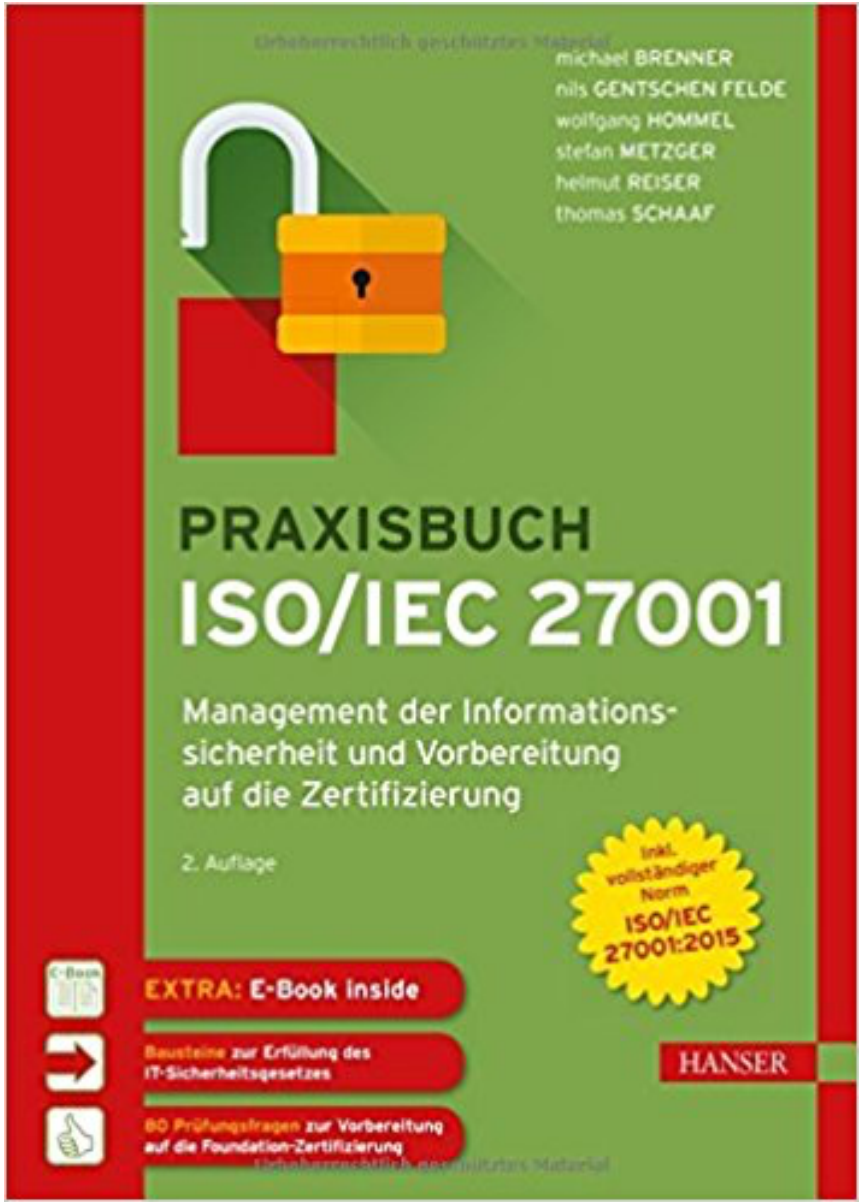
Literatur: IT-Sicherheit



- 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

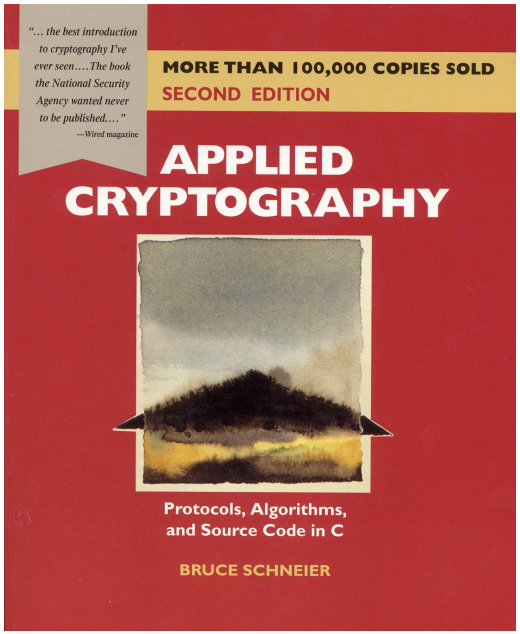
2. Auflage

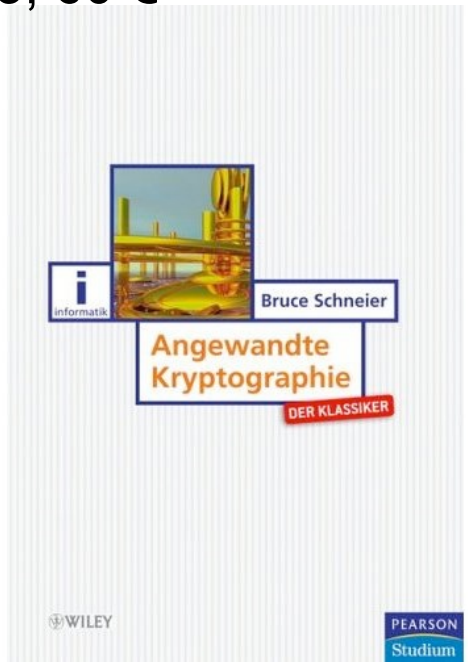
Hanser, 2017

64 €

Literatur: Kryptologie

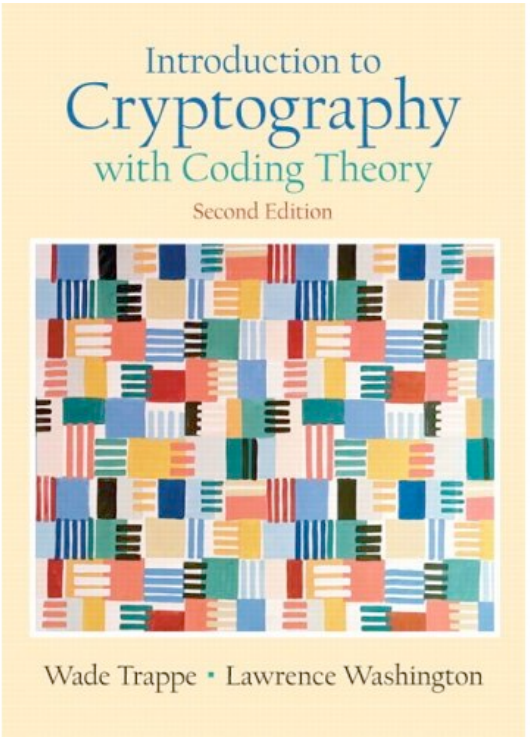
- Bruce Schneier
  Applied Cryptography
  John Willey & Sons, 20. Auflage
  2017
  69 €
  Angewandte Kryptographie
  Pearson Studium, 2005
  ISBN 3827372283, 60 €





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:
  - Introduction to Power-Aware HPC (Prof. Dr. Kranzlmüller, Dr. Hayk Shoukurian)
    Mittwochs 10:00 – 12:00, Amalienstr. 73A, Raum 220
    http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2020ws/powerhpc/
  - Introduction to Modern Cryptography (Prof. Dr. Kranzlmüller, Prof. Dr. Rührmair, Dr. T. Guggemos, S. Grundner-Culemann)
    Montags u. Donnerstags 10:00 - 12:00
  - Grid und Cloud Computing (Prof. Dr. Kranzlmüller, Dr. J. Watzel, M. Hab)

Weitere Veranstaltungen in diesem Semester

- Seminare:
  - Hauptseminar und Proseminar:
    Emerging Topics in ML & AI (Prof. Dr. Kranzlmüller, Dr. Luckow, M. Höb)
  - Hauptseminar: Physikalische Aspekte in Kryptographie und IT-Sicherheit
    (Profs: F. Gerfers (TU Berlin), D. Kranzlmüller, T. Lohmüller ,U. Rührmair, U. Schollwöck, J.-P. Seifert (TU Berlin), R. Thewes (TU Berlin), V. Tresp, H. Weinfurter, T. Weitz) Dr. T. Guggemos, S. Grundner-Culemann
  - Seminar und Praktikum: Wissenschaftliches Arbeiten und Lehren (Prof. Dr. Kranzlmüller, Dr. Schiffers)

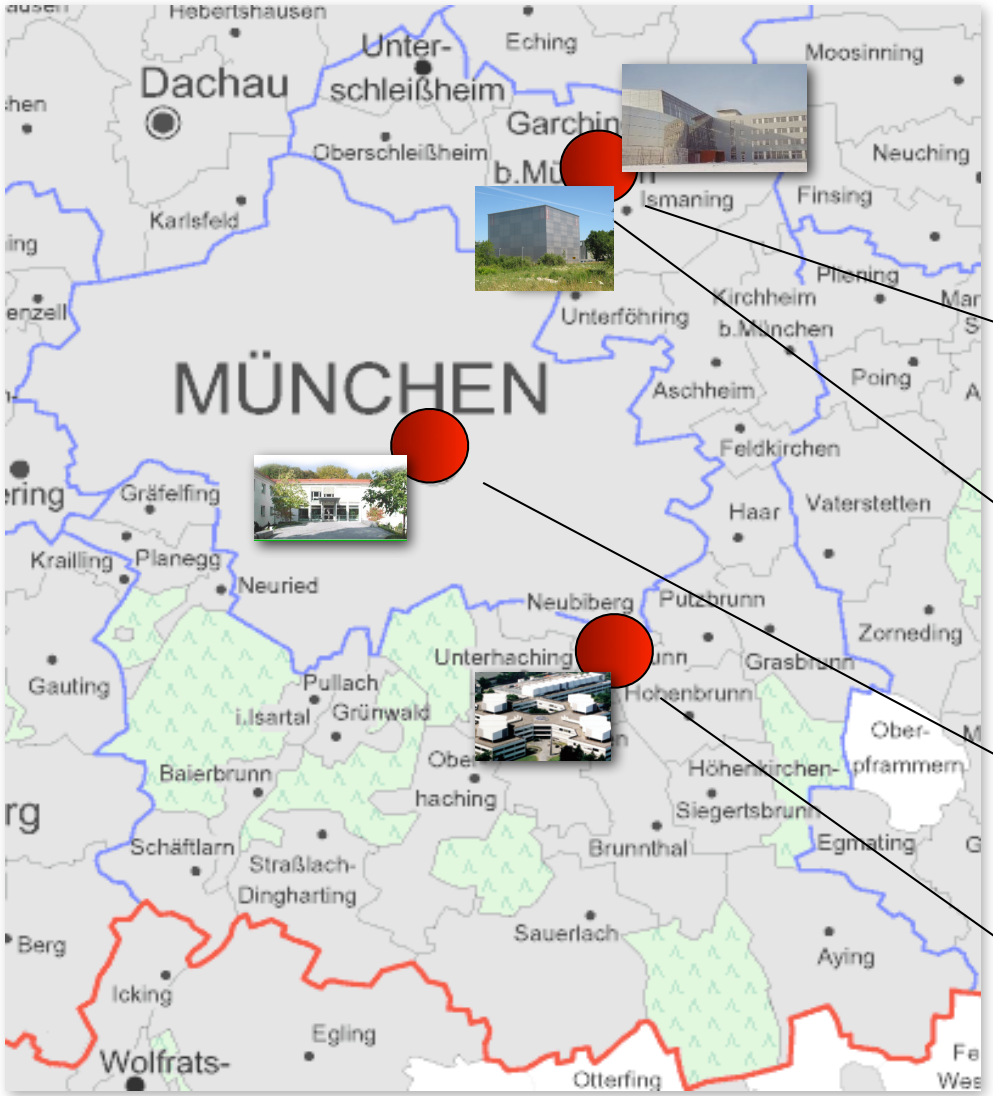
Weitere Veranstaltungen in diesem Semester

- Praktika:
  - Quantencomputing
  - Systempraktikum
  - Quantitative Analyse von Hochleistungssystemen
  - 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