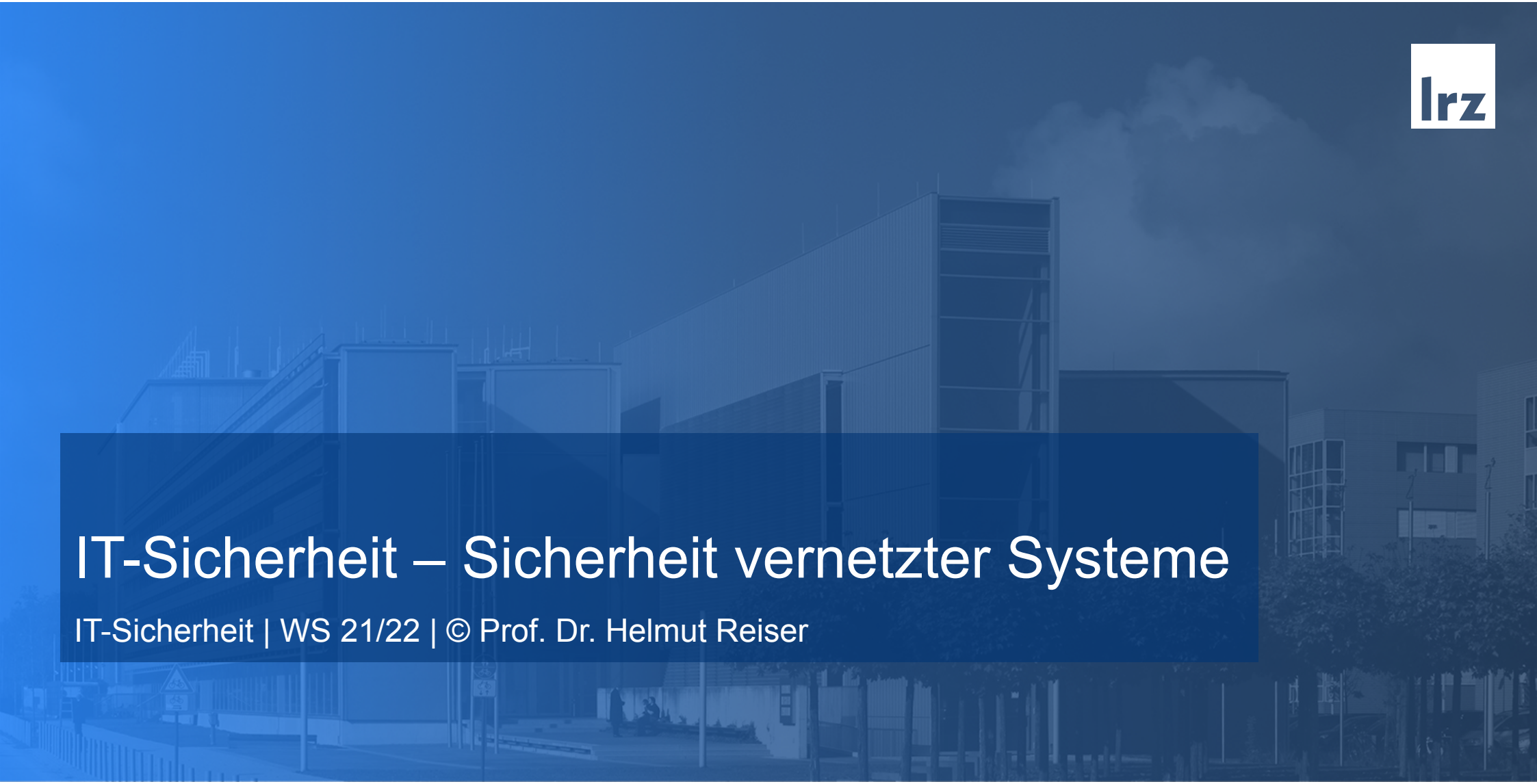

lrz
Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften



IT-Sicherheit – Sicherheit vernetzter Systeme

IT-Sicherheit | WS 21/22 | © Prof. Dr. Helmut Reiser

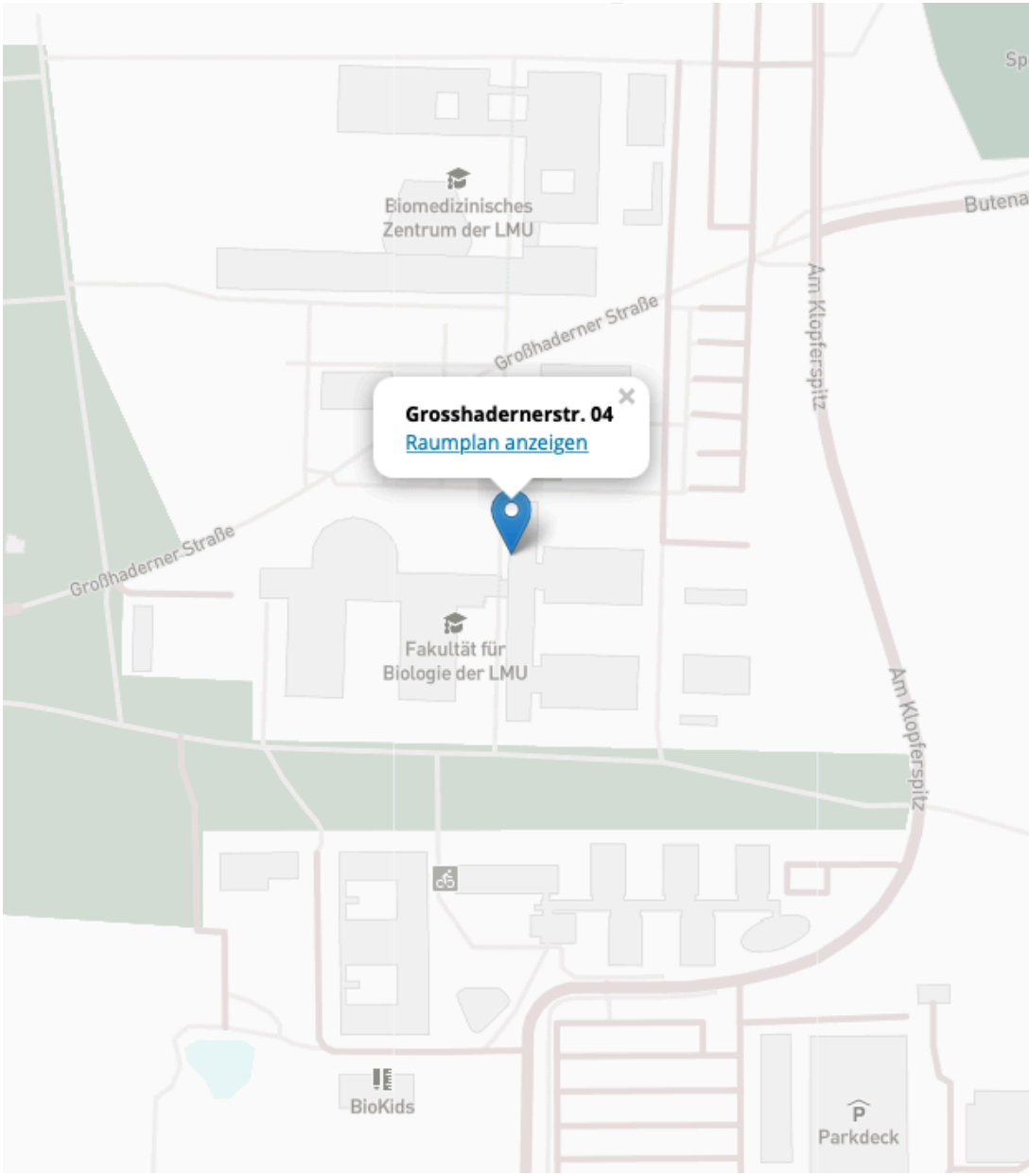
Regeln zum Infektionsschutz (Covid-19)

- Besucher der Vorlesung **sind** zu unterweisen

- Maskenpflicht (medizinische Maske, alternativ FFP2)
  - unabhängig vom Inzidenzwert: Maskenpflicht an der LMU
  - Wenn Abstand <= 1,5 m nicht eingehalten werden kann - auch in der Vorlesung

- Inzidenz > 35: Teilnahme an der VL nur mit 3G: Geimpft, genesen oder getestet
  - Kontrolle an den Eingängen oder Stichproben
  - Kostenlose Testmöglichkeit:
    - Schellingstraße 3 (gleich um die Ecke)
    - Martinsried, Großhaderner Str. 4
    - Buchung **ausschließlich** online: https://schnelltest-lmu.de

Teststationen



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

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
   - ❑ Ausgewählte technische Angriffsvarianten, z.B.:
     - ● Denial of Service
     - ● Schadsoftware (Malicious Code, …)
     - ● E-Mail-Security
     - ● Systemnahe Angriffe (Buffer Overflow, …)
     - ● 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

- 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 26.10.21
  - Dienstags von 12 - 14 Uhr als Online Veranstaltung
  - Übungsleitung:
    Stefan Metzger, metzger@lrz.de, Miran Mizani, miran.mizani@lrz.de, Michael Schmidt, michael.schmidt@lrz.de und Daniel Weber, daniel.weber@lrz.de
- Skript:
  - Kopien der Folien (pdf) zum Dowload
  - http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2021ws/itsec/
- Kontakt:

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

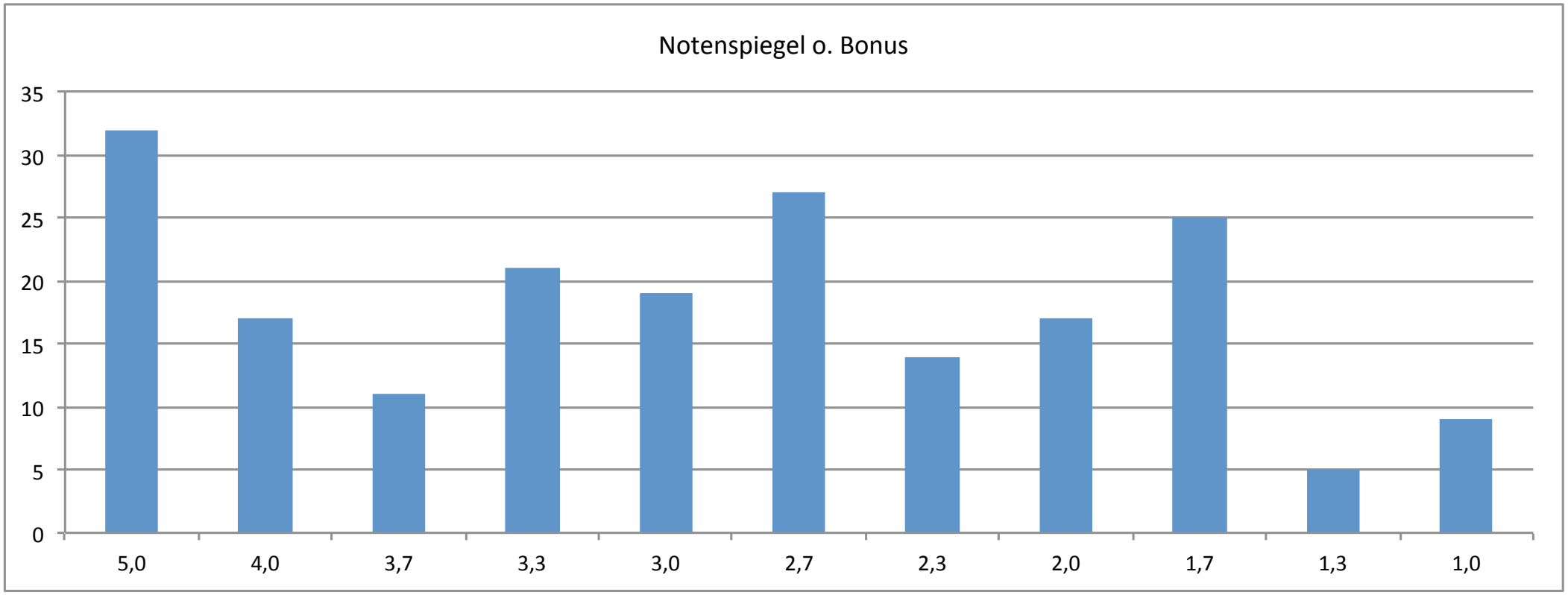
- Sprechstunde:
  nach der Vorlesung oder nach Vereinbarung im LRZ

Schein

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

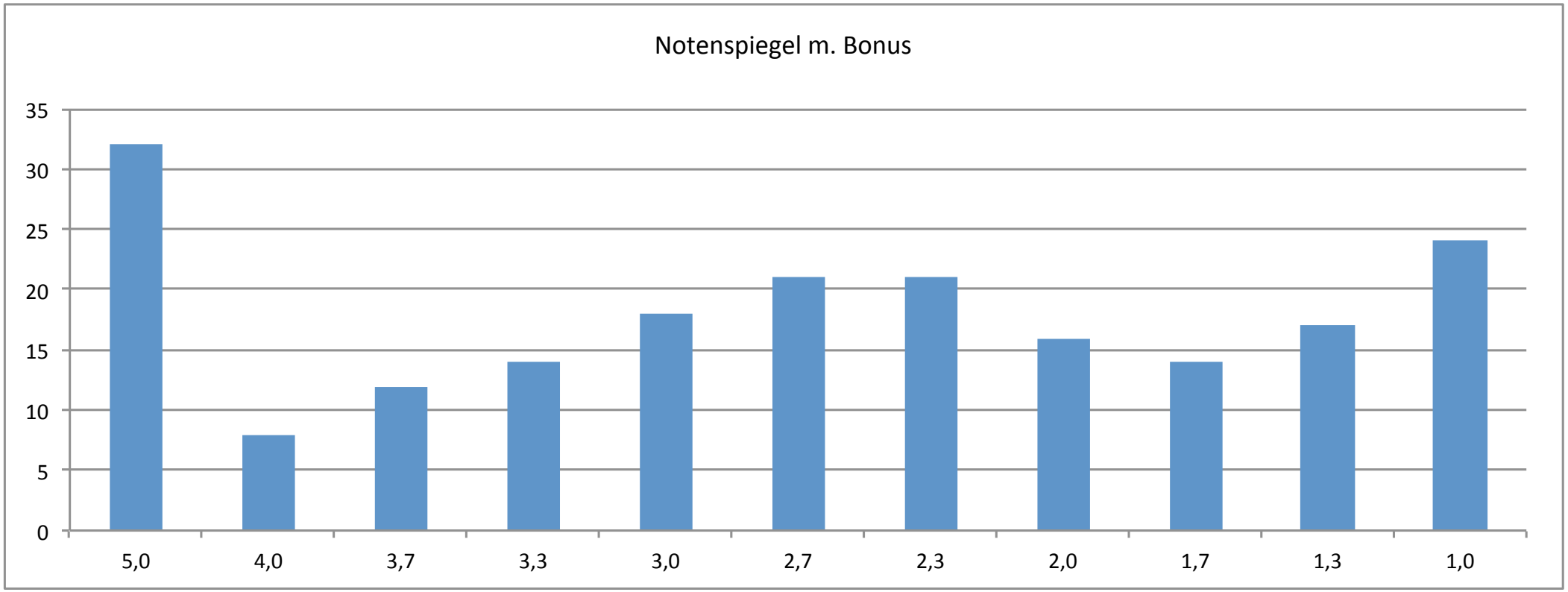
Notenbonus durch Hausaufgaben: Motivation

- Ergebnisse der Klausur WS15/16

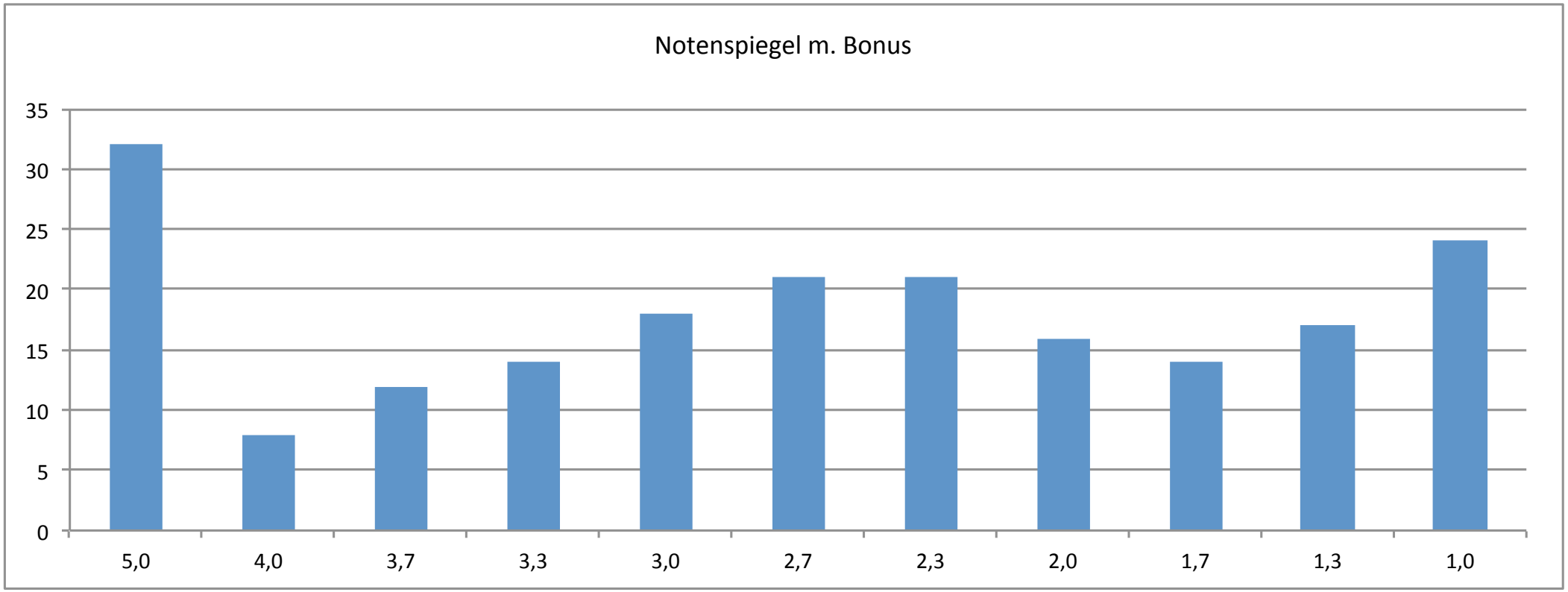


Notenbonus durch Hausaufgaben: Motivation

- Ergebnisse der Klausur WS15/16



Ergebnisse der letzten Klausur



Übung: Hausaufgaben aber kein Notenbonus

- (T) Tutoraufgaben
  - Vorbereitung
  - Musterlösung im Tutorium

- (H) Hausaufgaben
  - Selbständig zu Hause vorbereiten
  - Keine Korrektur, kein Notenbonus
  - Evtl. Fragen per Mail an uebung-itsec@lrz.de
  - Klausurrelevant -> Bearbeitung sinnvoll und ratsam

- **KEIN** Notenbonus in der Klausur

IT-Sicherheit

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

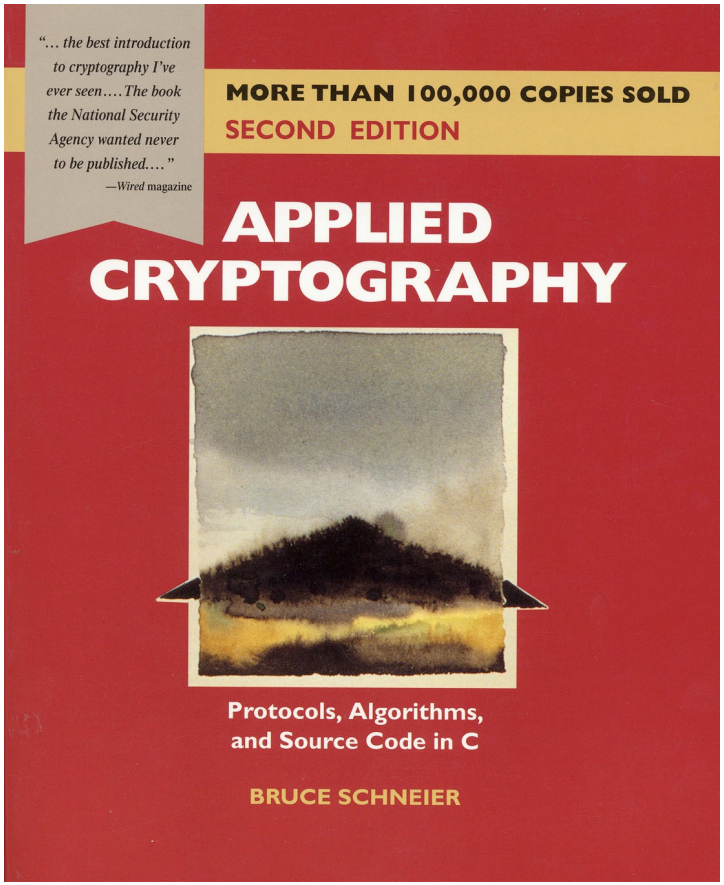
https://opacplus.ub.uni-muenchen.de/search?bvnr=BV040785275

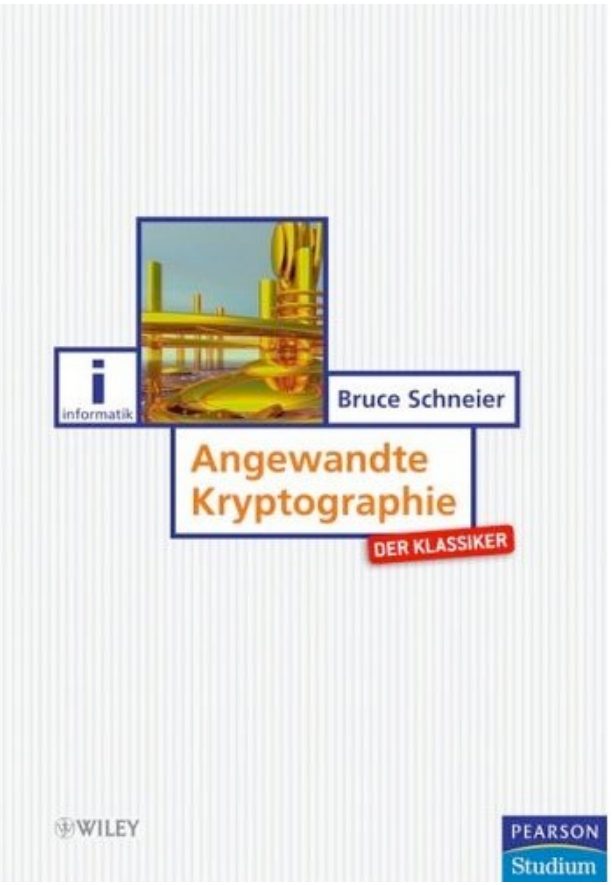
IT-Sicherheit

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
3. Auflage
Hanser, 2020
69,99 €

Kryptologie

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

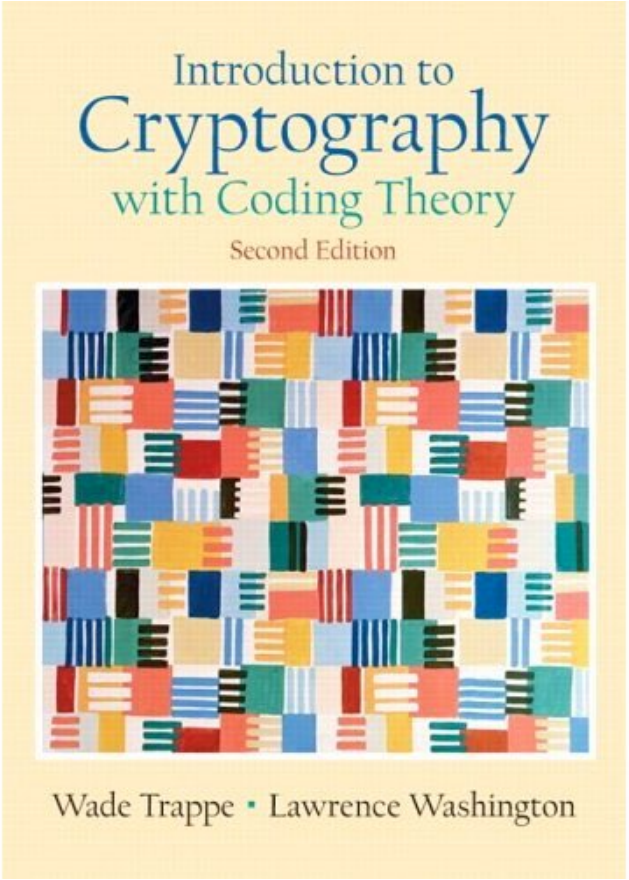




https://opacplus.ub.uni-muenchen.de/search?bvnr=BV021569735

Kryptologie

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. Karl Führlinger)
    https://www.nm.ifi.lmu.de/teaching/Vorlesungen/2021ws/Parallel/

Weitere Veranstaltungen in diesem Semester

- Seminare:
  - Hauptseminar und Proseminar:
    Emerging Topics in ML & AI (Prof. Dr. Kranzlmüller, Dr. Luckow, Dr. Fürlinger, M. Höb)
  - Evaluierung moderner HPC-Architekturen und -Beschleuniger (Dr. Fürlinger, M. Chung)

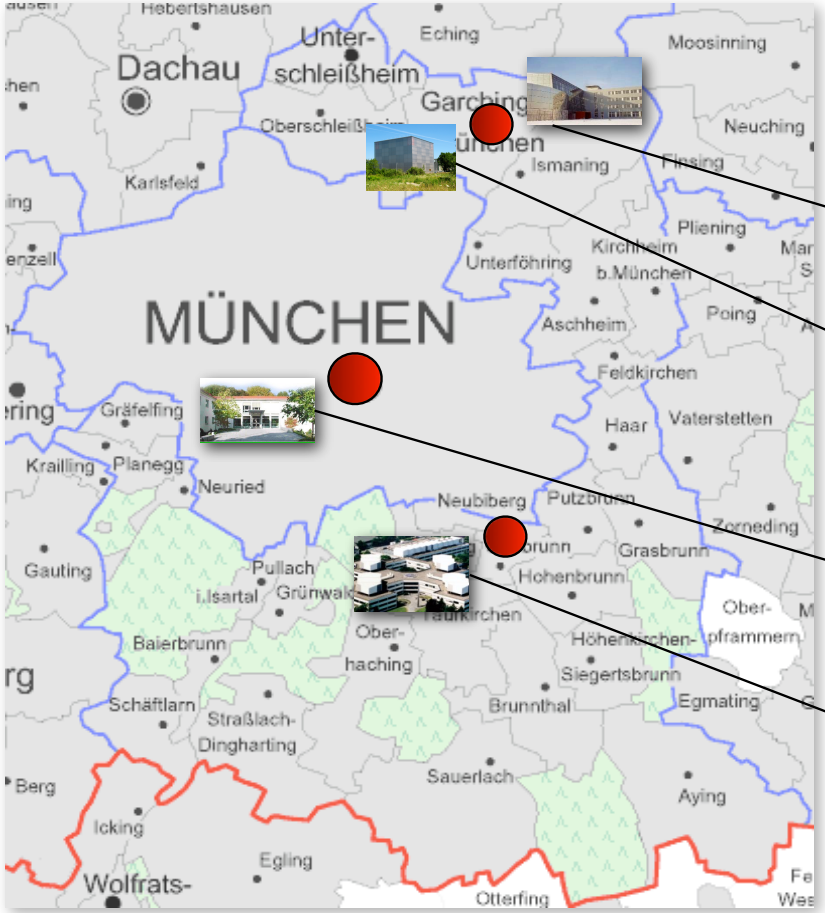
Weitere Veranstaltungen in diesem Semester

- Praktika:
  - Quantencomputing
  - Systempraktikum
  - Evaluation moderner HPC-Architekturen und -Beschleuniger

- 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