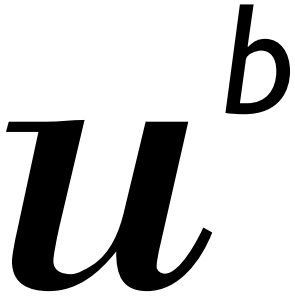

b

UNIVERSITÄT
BERN

UNIVERSITÄT
BERN

Network Security

Overview

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 21.02.2022

UNIVERSITÄT BERN

Contact

Prof. Dr. Torsten Braun

Address
Institut für Informatik
Universität Bern
Neubrückstrasse 10 (N10)
3012 Bern
Room 201

currently: Muesmattstrasse 27, Room -113

Contact
Phone: 031 684 4994
Email: torsten.braun@inf.unibe.ch
WWW:
http://www.cds.unibe.ch/about_us/team/current/prof_dr_braun_torsten

UNIVERSITÄT BERN

Network Security

Lecture and Exercises

Lecture and Exercises

- Location:
  Seminarraum S 201, UniS
- Date: Monday, 10-13 h
  except April 18, 2022 (Easter Monday)
- Material is available via ilias.unibe.ch.
- Course registration via
  mcs.unibnf.ch/admin until March 1, 2022

Responsible Assistants

- Dimitrios Xenakis
  (Phone: 031 511 7631),
  dimitrios.xenakis@inf.unibe.ch)
- Maria Hrabosova

UNIVERSITÄT BERN

Network Security

Exam

- Date: Monday, June 13, 2020, 10:15-11:15 h
- Location: UniS, Room A-126
- Admission to exam if 60 % of the exercise points have been achieved
- Registration via mcs.unibnf.ch/admin

UNIVERSITÄT BERN

Network Security

Focus of Lecture

- Encryption (symmetric, asymmetric) of data
- Data integrity algorithms to protect messages from alteration
- Authentication protocols to authenticate identity of entities
- Application of security mechanisms in the (wireless) Internet

- Lecture inspired by http://www.ccs.neu.edu/home/noubir/Courses/CS6740/F18/

UNIVERSITÄT BERN

Network Security

Textbooks

- William Stallings: Cryptography and Network Security, 8th edition, Prentice Hall
- Charles Kaufman, Mike Speciner, Radia Perlman: Network Security: Private Communication in a Public World, 3rd edition, Prentice-Hall
- Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography, 3rd edition, Chapman & Hall/CRC

UNIVERSITÄT BERN

Network Security

Chapters

1. Introduction
2. Symmetric Encryption
3. Asymmetric Encryption
4. Random Numbers and Hashing
5. Key Management
6. Authentication Protocols
7. Wireless Networks
8. IP Security
9. Cellular Networks
10. Transport Level Security
11. Electronic Mail and Domain Name System
12. Network Endpoint Security

UNIVERSITÄT BERN

Communication and Distributed Systems

Research Projects and Topics

- Machine Learning in Networking
  - Mobility Prediction
  - Indoor Localization
  - Federated Machine Learning
- Future Internet
  - Information- and Service-Centric Networking
  - Recursive Internetwork Architecture
- Network Function Virtualization
  - Mobile Edge and Fog Computing
- Networking for Immersive Communications

Thanks

for Your Attention

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 21.02.2022