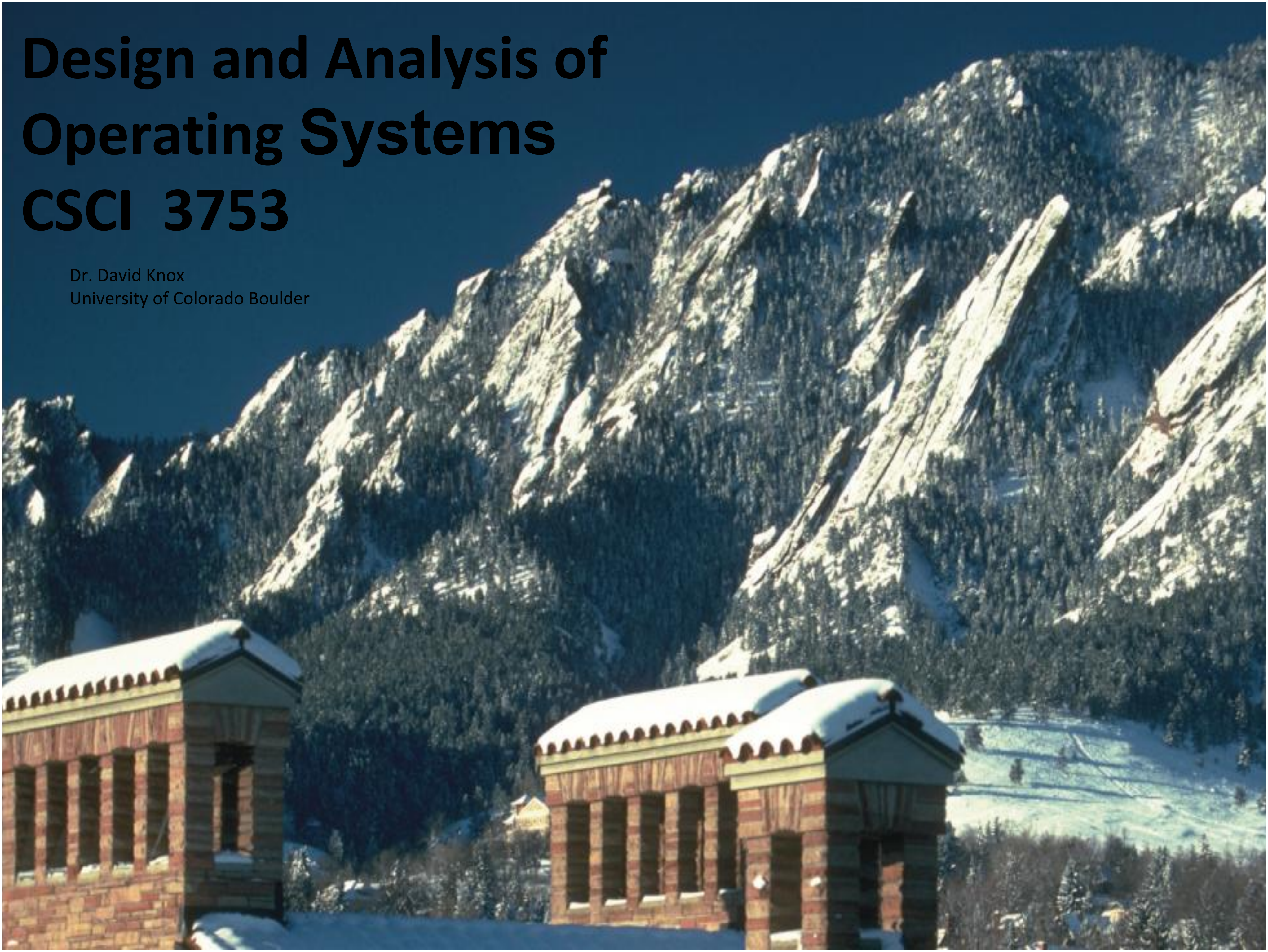
Design and Analysis of Operating Systems CSCI 3753

Dr. David Knox
University of Colorado Boulder



Design and Analysis of Operating Systems CSCI 3753

Security in Operating Systems

Dr. David Knox

University of
Colorado Boulder

Security in Operating Systems

Non-repudiation

Availability

6 Main Areas of Security

1. *Authorization* – managing access to resources
2. *Confidentiality* – only allow authorized viewing of data - encrypting files and communication
3. *Authentication* – proving you are who you say you are
4. *Data Integrity* – detecting tampering with digital data
5. *Non-repudiation* – proving an event happened
6. *Availability* – ensuring a service is available
(despite denial of service attacks)

Non-repudiation

- **In digital security, non-repudiation means:**
  - Involves associating actions or changes with a unique individual
  - A service that provides proof of the integrity and origin of data
  - An authentication that can be said to be genuine with high confidence.

- **Usually requires:**
  - Authentication
  - Authorization
  - Data Integrity
  - Confidentiality

6 Main Areas of Security

1. ***Authorization*** **– managing access to resources**
2. ***Confidentiality*** **– only allow authorized viewing of data - encrypting files and communication**
3. ***Authentication*** **– proving you are who you say you are**
4. ***Data Integrity*** **– detecting tampering with digital data**
5. ***Non-repudiation*** **– proving an event happened**
6. ***Availability*** **– ensuring a service is available**
   (despite denial of service attacks)

Denial-of-service attacks (DoS)

Designed to make data, a machine, or network resource unavailable to its intended users

- **Denial-of-service attacks (DoS)**
  - Either a single source or distributed attack to prevent access by authorized users
- **Direct-access attacks**
  - An unauthorized user gaining physical access to a computer
- **Tampering**
  - malicious modification of information

Denial-of-service attacks (DoS)

Designed to make data, a machine, or network resource unavailable to its intended users

- **Eavesdropping**
  - act of surreptitiously listening to a private conversation, typically between hosts on a network
- **Phishing**
  - attempt to acquire sensitive information such as usernames and passwords
- **Privilege escalation**
  - attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level
- **Spoofing attack**
  - Spoofing is the act of masquerading as a valid entity through falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain

Department of Computer Science
UNIVERSITY OF COLORADO **BOULDER**

Design and Analysis of Operating Systems CSCI 3753

Dr. David Knox

University of Colorado Boulder

Material adapted from: Operating Systems: A Modern Perspective : Copyright © 2004 Pearson Education, Inc.