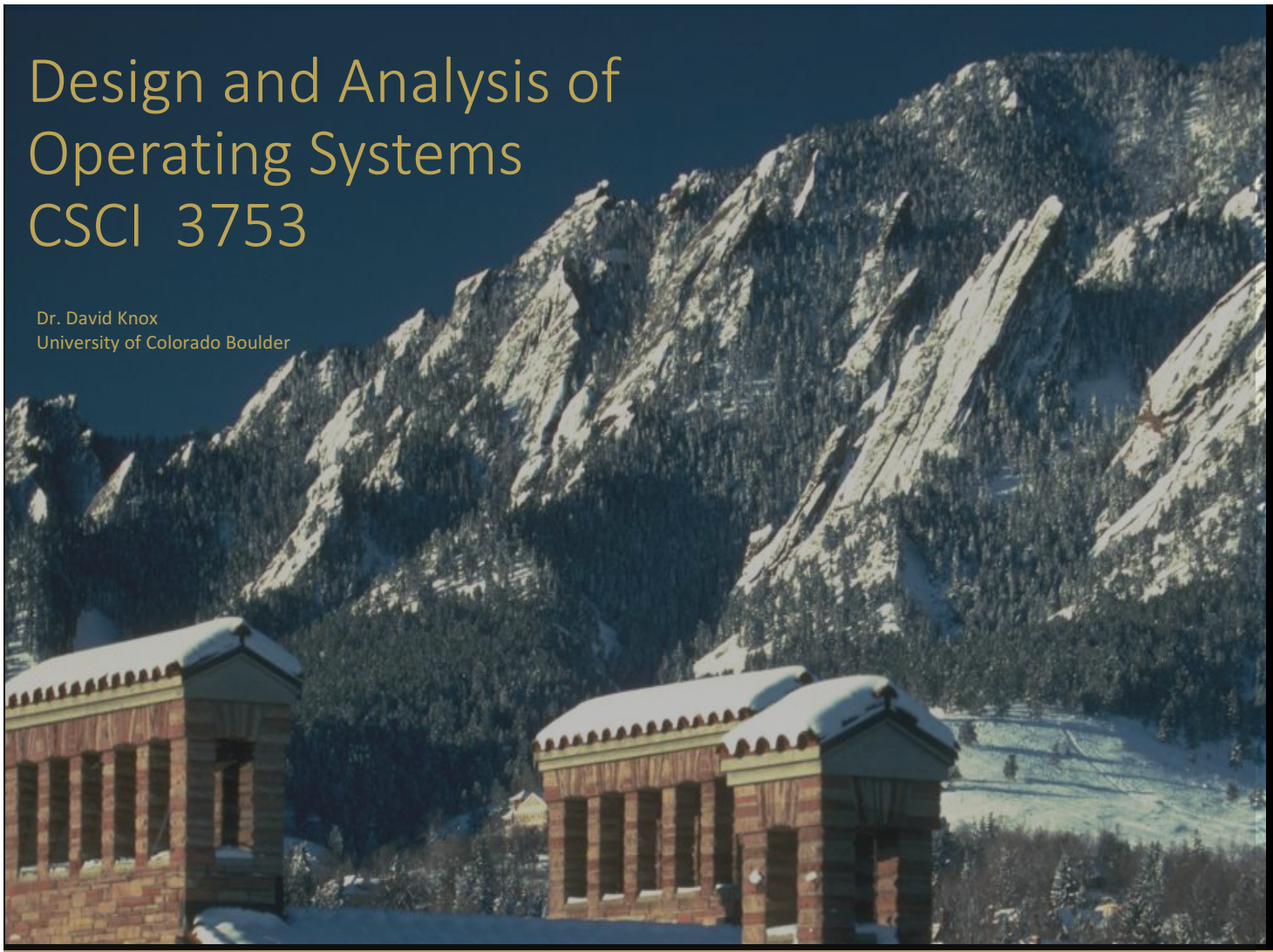
Department of Computer Science
UNIVERSITY OF COLORADO BOULDER

Design and Analysis of Operating Systems CSCI 3753

Dr. David Knox
University of Colorado Boulder

These slides adapted from materials provided by the textbook authors.

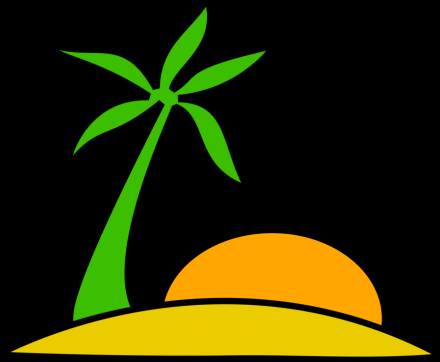
Design and Analysis of Operating Systems CSCI 3753



Dr. David Knox
University of Colorado Boulder

Security

Security



Security

1. *Authentication* – proving you are who you say you are, e.g. passwords
2. *Authorization* – managing access to resources, e.g. files
3. *Confidentiality* – only allow authorized viewing of data - encrypting files and communication
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)

Authentication

- Prove you are who you say you are
  - e.g. Logging into your laptop or smartphone
- Password is a form of authentication
  - Providing the correct password is seen as authenticating the user to the OS
- New: biometric authentication on smartphones
- For text-based authentication:
  - Attacker can try to guess your password, using common words, etc.
  - OS can block or slow down access after too many login attempts

Remote Authentication

- Harder than logging into your own laptop/mobile phone
- Now must communicate login messages over the network
  - Early *rlogin* sent password unencrypted!
  - An attacker can employ a *replay attack*: just replay the password to login as the intercepted user
- Should encrypt the password!
  - *But even an encrypted password can be replayed!*

Other Authentication Approaches

- Challenge-response protocol:
  - X and Y share a secret symmetric key. X wants to authenticate a node N that says it is Y.
  - X sends a challenge to N, i.e. a random number used only once
  - N sends to X nonce encrypted w/ N's symmetric key
  - X decrypts N's message with X's sym key. If decrypted # matches nonce, X knows responder N is Y.
- 1-time password
  - a list of one-time passwords is generated a priori and then consulted during login at both ends
  - list could be generated using a one-way function

Defense In Depth

- Standard security philosophy is *defense-in-depth*
  - employ multiple layers of security
- For each layer, identify:
  - What is the threat model?
    - e.g. eavesdropping, replay, MIM, DDOS, etc.
  - What resources does the attacker have available to them?
    - One attacker or many?
    - A laptop or a supercomputer?
  - What resources do you have to defend at that layer?

Relevance of security to operating systems:

- Users have to provide a password to login
  - this is a form of *authentication*
- OS must keep track of rights a user has to each file, object, and service
  - this is a form of *authorization*
- Some data is sensitive and be encrypted.
  - this is a form of *confidentiality*.
- Networked services to remote users may invite malicious adversaries
  - may wish to prevent access to these services, engaging in distributed denial-of-service attacks (DDOS)
  - this is a form of *availability*.
- Detect whether data has been tampered with.
  - this form of *data integrity*.

Department of Computer Science
UNIVERSITY OF COLORADO BOULDER

Design and Analysis of Operating Systems CSCI 3753

Dr. David Knox
University of Colorado Boulder

These slides adapted from materials provided by the textbook authors.