

Overview of Authentication Systems

Raj Jain

Washington University in Saint Louis
Saint Louis, MO 63130

Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

<http://www.cse.wustl.edu/~jain/cse571-09/>



- ❑ Passwords
- ❑ Address based authentication
- ❑ Key Distribution Center (KDC)
- ❑ Certification Authorities (CAs)
- ❑ Multiple Trust Domains
- ❑ Session Keys
- ❑ Delegation

Passwords

- ❑ Do not store passwords in clear. Store hashes.
⇒ Subject to offline attack
- ❑ Encrypt the hash storage.
⇒ Where do you keep the master key?
- ❑ Do not transmit passwords in clear.
- ❑ Use password as a key to encrypt a challenge.
⇒ Cryptographic Authentication