Unix System Administration

Chris Schenk
Lecture 20 – Tuesday Apr 03

CSCI 4113, Spring 2007

Logistics

- Avenade talk tonight after class in ECCR 155
  - Free food from what I understand
- Guest talks from other sysadmins
  - Chris Triolo – Cybertrust
    - Security and vulnerability scanning
  - Matthew Woitaszek – Computational Science Center
    - Supercomputing and other bits
- Quiz 02 is long, don't start on it late!
- Moving back to security after email
  - Because it's interesting and cool

Cryptographic Hash Properties

- Cryptographic hashes have three general properties
- Preimage resistance
  - Given a hash value *h*, it is difficult to find the original message
- Second preimage resistance
  - Given a hash value *h* and it's message *m1*, it is difficult to find another input *m2* such that h = h(*m1*) = h(*m2*)
- Collision resistance
  - It should be difficult to find two messages *m1* and *m2* such that h = h(*m1*) = h(*m2*)