Security Systems
Lecture notes

Drs. Brian Tung and Clifford Neuman
University of Southern California
Information Sciences Institute

CSci530: Security Systems
Lecture 1 – August 27, 2003

Drs. Brian Tung and Clifford Neuman
University of Southern California
Information Sciences Institute

Administration

- Class home page
  - Syllabus
  - Reading list
  - Lecture notes
  - Assignments
  http://ccss.isi.edu/CSci530.html

Administration

- Class e-mail: csci530@usc.edu
  - Not yet working
- Instructors
  - Dr. Brian Tung
  - Dr. Clifford Neuman
- TAs (Department is still reassigning)
  - Jonathan Kelly
  - Ho Chung
- Office hours: To be Specified

Administration

- A separate 2 unit lab class is available as ITP-499 Advanced Security Systems
- Will be offered if 12 people sign up by today, as of yesterday only 3 registered.
- Provides hands on experience with systems discussed in class.
- Developed jointly with this class.

Administration

- Grading
  - Reading reports: 5,5,5
  - Exams: 25,40
  - Research paper, 20
  - Class participation (up to 10% bonus)
What is security

- System, Network, Data
- How to evaluate
- Security vs. Risk Management

What do we want from security

- Protection
  - Enforced by hardware
  - Depends on trusted kernel
- Authentication
  - Determining identity of principal
- Integrity
  - Authenticity of document
  - That it hasn't changes
- Privacy
  - That inappropriate information is not disclosed

What makes up security

- Authentication
- Authorization
- Accounting
- Audit
- Assurance
- Payment
- Protection
- Privacy
- Policy
- Confidentiality

Security weaknesses

- Buggy code
- Protocols design failures
- Weak crypto
- “Social engineering”
- Misconfiguration
- Incorrect policy specification
- Stolen keys or identities
- Denial of service

Security mechanisms

- Encryption
- Key management
- Authentication
- Authorization
- Accounting
- Firewalls
- VPNs
- Intrusion detection and response
- Development tools
- Virus Scanners

Today’s security deployment

- Most of the deployment of security services today handles the easy stuff, implementing security at a single point in the network, or at a single layer in the protocol stack:
  - Firewalls, VPN's
  - IPSec
  - SSL
- Unfortunately, security isn't that easy. It must be better integrated with the application.
  - At the level at which it must ultimately be specified, security policies pertain to application level objects, and identify application level entities (users).