Security Policies for Large Systems
CS 239
Security for Networks and System Software
May 7, 2002

Security Policies

- Who is allowed to do what when
- And what happens if they do something else
- And who's responsible for making sure that's done, if needed
- And what to do if something goes wrong

More Formally,

- A security policy is a written statement that describes an organization's approach to securing its computer assets
- Useful for many purposes

What Should a Security Policy Cover?

- Who are the legitimate users?
- What are the assets being protected?
- Who has what responsibilities for security?
- What is appropriate use of the system?
- What are the consequences of inappropriate use?

Getting Down to Brass Tacks

- The UCLA Computer Science Department doesn't have a formal security policy
- I think it should
- What should it be?

Some Details on the Department Facility

- Meant to support CS department needs
  - Research
  - Education
  - Administration
- No service provided to other departments

Types of Users

- Faculty and lecturers (58)
- Staff (26)
- Graduate students (343)
- Guests (21)
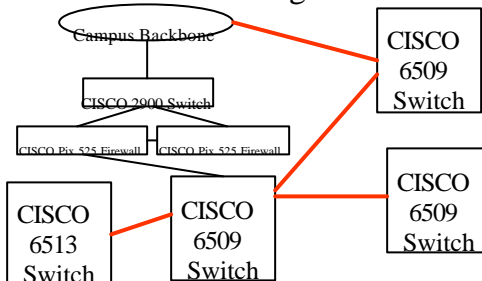- Nobody else should have access
  - Except to web sites

Machines on the Network

- Sun machines – 220
- Intel-based PCs – 450
- Macintoshes – 30
- HP, SGI, Digital workstations – 21
- PDAs – 50
- Several printers
- Scanner

Network Configuration

Campus Backbone

CISCO 6509 Switch

CISCO 2900 Switch

CISCO Pix 525 Firewall   CISCO Pix 525 Firewall

CISCO 6513 Switch   CISCO 6509 Switch

CISCO 6509 Switch

Our Wireless Network

- 802.11 equipment
- Covers essentially all of the 3d and 4th floors of Boelter Hall
  - With a little "spill" elsewhere
- Currently uses both static IP addresses and DHCP
  - DHCP use requires registered HW address for wireless card

What Kind of Data Do We Store?

- Lots of research data
- Some class-related data
- A fair amount of administrative data
  - Much critical stuff in other systems
  - But things like the CS web site are under our control

Our Staff

- Pete Follett
- Steve Sakamoto
- Peter Schultze
- Charlie Fritzius
- Often part-time student helpers
- I'm the faculty contact for the facility

What Are We Protecting?

What Are Our Priorities?

What Are the Users' Security Responsibilities?

What Is Appropriate Use?

What Are the Consequences of Inappropriate Use?

A Special Question for Us

- What about the labs that run their own networks and systems?