CS 107 Fall 2006
Chapter 11: Security

1 Data Security: PAPA and the CIA

PAPA and CIA are acronyms to help us remember the kind of security we need. PAPA stands for

- Privacy: Data must be kept out of the hands of spies and enemies.
- Accuracy: How do we know that the contents of the file have not been changed?
- Protection: The file must be protected from deletion.
- Availability: When we need the data, we must not be blocked from reaching it. Even if we have backups, they may be a day or a week old, and they may not be immediately available.

CIA stands for Confidentiality (like privacy), Integrity (a combination of protection and accuracy) and Availability.

2 Security from the Ground Up

- Physical premises control.
- Control over access to system through wireless and/or internet: firewalls, closed ports
- File ownership and permissions.
- Passwords and authentication. A real problem in lab environments where the files live centrally and can be accessed from any workstation.
- Insider fraud.
- Social engineering.

3 Who is the Enemy?

- Hooligans: Want to prove how clever they are. Like doing secret illegal things. Don't consider other people.
- Terrorists: Who wants to shut down the power grid; take over Air Traffic Control, etc.
- Corporate and governmental spies
- People who can gain money or power. (Mafia, politicians.)
  - Voting fraud
  - Scams
  - Stock market manipulation
- Angry employees or former employees. Accounts are normally deleted immediately.
- Would-be saviors: IT departments, "white-hat" hackers?
- Experts who say there is no problem.

4 Designing for Security

- Security through Obscurity: Why it doesn't work; who's smart, who's stupid?
- Using Responsible Design and Programming Practices Buffer overflow problems happen because programmers are either ignorant or lazy.
- It's a Game
  The defenders move first, the attackers find a way to defeat defenses. Repeat.
- Planning Through Attack Scenarios
  Think of a threat, think of how to defend against it. Repeat.

5 Increasing your own security

- Windows. Microsoft frequently develops patches to fix bugs. Be sure to set option that permits Microsoft to automatically inform you of these updates.
- Firewalls - Install a firewall, antivirus and anti-spyware programs
- File systems - make backups, encrypt important files, set file access permissions and clean up regularly. Choose a good password.
- Email - set spam filters. Watch out forworms, don't fall for hoaxes
- Watch out for phishing. Check the URL on a link (hold mouse over it) and be sure it matches the text in email.
- Wireless - turn off SSID broadcast, limit connections by MAC addresses, reset default admin password, set encryption type to WPA, watch out for viruses that infect you through your cell phone or somebody else's ipod.
- Downloads. Any site that will let you download copyrighted or illegal information is likely to transmit viruses also. Spyware is downloaded when you visit the "get something for nothing" sites.