Introduction & Goals

COMP620 Information Privacy and Security

What is Computer Security?

“Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as “intruders”) from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.”

United States Computer Emergency Readiness Team

Personal Concern

"Forty-one percent in the U.S. and 38 percent in the U.K. said security was a most important reason for not banking online."

Gartner Survey – June 2009

Corporate Concern

"Understanding corporate security is about understanding what the key assets in the company are. Today, the key asset is often information."

An Overview of Corporate Information Security

By Seán Boran

National Concern

- “ABC News reports that the Department of Energy may jeopardize the security of its nuclear weapons and energy technology and lose millions of dollars if it does not improve its cyber security, according to a recent Inspector General’s report.”

Homeland Security Daily Open Source Infrastructure Report for 24 December 2009

Who is Hacking?

- The media once promoted the idea of an adolescent geek working in his basement easily breaking into corporate and government computers just for the fun of it

Follow the Money

- Most computer criminals do it for the money
- Steal information (such as credit card numbers) to be sold for profit
  - Social engineering
  - Exploitation of vulnerabilities
- Extortion
- Installing malicious software to use victim computers as "bots" in a larger attack
- Change information *(your grades)*

Cyber War

- Nations are very concerned about an enemy attacking the country's infrastructure
- The impact of a well organized attack could be serious
- The Estonian Cyberwar (Web War 1) refers to a series of cyber attacks that began April 27, 2007
  - Russia was angry at Estonia about the relocation of a Soviet-era grave marker

Security Goals

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Anonymity

Privacy

- We want to prevent:
  - Someone from impersonating you
  - Releasing information to someone that we do not want them to know
  - Providing information about our activities to people who do not need to know

Levels of Threat

The level of system security required depends upon the expertise of the attacker.

1. Ordinary web user
2. Sophisticated user *(CS students)*
3. Professional Thief
4. Insider
5. Corporate
6. Government

Cost of Security

- Security has a cost in hardware, software and user convenience
- The cost of defeating a security system must be greater than the value of the data it protects

The Big Players

- Department of Homeland Security **(DHS)**
- National Cybersecurity and Communications Integration Center's **(NCCIC)**
- National Institute of Standards and Technology **(NIST)**
- Department of Defense **(DoD)**
  - National Security Agency **(NSA)**
- International Standards Organization **(OSI)**

Protecting Ourselves

- Some authors talk of a “war” between the black hats and the white hats
- When the “bad guys” discover a new vulnerability, the “good guys” scramble to correct the problem.
- There will probably always be security threats.