Security

The Individual and the Enterprise

• Two lectures on security
• Today: Focus on how individuals can protect themselves
• Later: Enterprise security
Need to Protect

• Information
• Hardware
• Software
• Access
  – Availability to authorized users
  – Limit access to unauthorized users
• Your accounts (e.g., spam)

Malware

• *Malware*: Malicious software
• Viruses
• Worms
• Trojan Horses
  – Not infectious
  – Harmful
Viruses

- Attach themselves to a host program
- When the host program is run by the user
  - Virus infects computer and other suitable programs when they run
    - Self-replicating
- User must act for virus to take effect

Viruses

- Frequently spread through email
  - Replicate by emailing themselves to other people in user’s address book
  - Messages include infected attachments
- Also the WWW
  - Pop-up windows in some web sites
Worms

• Exploit vulnerabilities on networked computers
  – Worm installs itself without user intervention
    • Self-replicating
  – Important reason to update OS frequently

• Common payload is to install a backdoor
  – Way to access computer without authentication
  – Turns computer into a “zombie” under control of worm author
  – Networks of zombies: botnets

• Worms don’t always have a payload
  – Sometimes written as pranks or for research purposes
  – Still harmful: generate network traffic
Trojan Horses

• Disguised as innocuous or desirable software
  – Must be run to take effect
  – Not self-replicating

• Common effects
  – Introduce virus into a computer
  – Steal information
  – Set up a zombie computer as part of botnet
  – Set up an anonymous computer to hide Internet usage

For-Profit Malware

• Infect computers to make money
• Spyware
• Botnets
• Keystroke loggers
Spyware

• Program placed on a computer that collects personal information
  – Web browsing habits for advertisements
  – Financial information

• Main problems
  – Invasion of privacy
  – Degradation of system performance
  – Unwanted pop-up ads

Spyware

• Installed through:
  • Deception
    – Bundled with other software (e.g., P2P)

• Security holes in a Web browser

• Not self-replicating
**Botnets**

- Collection of zombie computers under control of one bot server
- Several possible uses, some malicious
  - Spam
  - Denial of Service attacks against enterprises
  - Obtain personal or confidential corporate information

**Keystroke Loggers**

- Track the keys struck on keyboard
  - Hardware-based
  - Software-based
    - Includes screen loggers and clipboard loggers
Keystroke Loggers

- Uses are both malicious and within the law
- Malicious
  - Passwords or PINs
  - Financial information
  - Personal information
- Within the law
  - Law enforcement
  - With user’s consent, use to improve the way web applications work

Protective Measures: Behavior

- Never open unanticipated email attachments
- Never respond to email messages asking for a password or PIN
- Do not start computer with USB drive, CD, or DVD in the machine
- Be careful with spreadsheets and other applications containing macros
Protective Measures: Safeguards

- Set computer to update the OS automatically
- Install an antivirus program
- Install a personal firewall
- Install a secure wireless system
- Do business only with secure web sites

Antivirus Programs

- Main line of defense: “signatures”
  - Pieces of computer code that are characteristic of particular malware
  - Virus signatures must be updated automatically
  - Need a contract with the company selling your AV program
- Some programs: heuristic scanning
  - Examines programs for suspicious behavior
Personal Firewall

• Operating system version
  – Windows Vista and 7 include firewalls
• Software version
  – Purchase application that serves as a firewall
• Hardware version
  – Purchase a router that includes a firewall

Wireless Security

• WiFi Protected Access (WPA)
  – Users must authenticate to use network
  – Encrypts wireless signal between computer and access point
  – Common on home systems
• 802.11i
  – More advanced encryption
  – Common in enterprise environments (e.g., Wofford)
Encryption

- Plaintext: data that is in readable form
- Ciphertext: data that has been encrypted
  - Basically a secret code

TLS and SSL

- Secure Sockets Layer (SSL)
  - Part of a security protocol named Transport Security Layer (TLS)
- Used by Web browsers and servers
- SSL encrypts transmission so that it cannot be read
- Very important when using the commercial Internet for financial or sensitive personal information
TTL and SSL

• When being used, URL includes **https://**
• Examples: Amazon.com checkout and myWofford

Secure Web Sites

• When making a financial or sensitive personal transaction over the web, look for evidence that site is secure
  • Padlock on web page
  • URL includes **https:**
  • Another example: myWofford