Topic 3: Computer Defense

Eric Mlinar
CS 6
4/4/2016
But first...

• Napster fall, copyright infringement
Google & P2P

1998
- Google founded.
- PageRank more important than database size
- Every country online

1999
- Napster: first widely used Peer to Peer (P2P) Network
- LiveJournal launched, makes blogging easy
• 2001
  • Seti@Home
  • Napster closed

• First webcam ever to broadcast shuts down (pointed at coffee pot since 1991)

• Wikipedia launched
Napster’s Example

• Napster fall, copyright infringement
• *To what extent is a product responsible for its use?*
• *Already a big discussion on this:*
• Weapons involved in interpersonal violence, yet gun companies are not held responsible
Interesting Topics

• Encryption, Privacy, and Security
• *San Bernardino shooting: FBI vs. Apple*
• Veracity of Wikipedia
• *Encyclopedia Britannica vs. Wikipedia*
• Copyright policy and protection
• *Napster, P2P, downloading, uploading*
• WikiLeaks (discussion)
• SOPA (stop online piracy act)
• And other internet regulation
Review
Topic 3: Computer Defense

Eric Mlinar
CS 6
4/4/2016
Backup Your Data

• The first rule of computers: always backup your data.

• The second rule of computers: always backup your data.

• …If you learn nothing else…

 BACKUP YOUR DATA
How to Backup

• Many ways!
• *Windows built-in service*
• All Programs / Accessories / System Tools / Backup
• Control Panel -> Search “backup”
• *Manually:*
  • Copy/paste “My Documents” folder (Pictures too?)
  • What are your important files?
• Burn a disk.
• Use “the Cloud”
Backup Drives

• Maxtor’s OneTouch drive ($80 - $300)
  • *Difference is the software, which Maxtor has gotten right*

• The cloud!
  • *Did you know: your R’mail account (a Gmail service) has unlimited storage on Drive?*
  • Dropbox
Why Backup?

• Virus
• Failed software install
• Power spike
• Disk crash
• Accidental deletion
• Soda spills
Know Thy Enemy

- **Viruses**: come as files that you download, mostly by email. Hurt your computer
- **Worms**: Self-propagating over networks, usually hurt networks
- **Trojans**: come hidden inside of other, apparently desirable software
- **Spyware**: collects personal information about users without consent
Zombies!

- Zombie computers
- *Computer is operated remotely without your knowledge, to do bad things*
Defense

• Don’t download from obscure websites
• Scan any files before installing
• Should be done automatically
• Don’t open files in an email unless you are already expecting it
• Even from a friend
Defense: Virus

- Viruses need **anti-virus software**
  - *AVG (Anti-Virus Guard), free!*
  - *Very good (actually what I use/recommend)*
- **NOD 32**
  - *Not free, but still recommended*
  - *Lightweight (and no ads)*
  - *Very, very good*
- **Avira AntiVir**
Defense: Virus

• Anti-virus is only as good as its definitions
• *Don’t use “better” outdated software*
• *Switch to AVG if nothing else*

• **ONLY RUN ONE ANTI-VIRUS**
  
  • *Multiple anti-virus programs actually cannibalize each other*
  
  • *Uninstall existing AV first (then install AVG)*
  
  • *Backup first! AV programs are sometimes a pain in the **** and can throw a fit*
Defense: Worms

- **Firewall** (sometimes in router)
  - *Barrier that watches any attempts to exit or enter your computer.*
  - *Attempts are blocked unless you give permission*
- Windows comes with firewall
  - *Only stops incoming attacks*
- ZoneAlarm has free version
Defense: Worms

• Routers
  • *Network hub, gateway to the internet*
  • *Absorb a lot of attacks (which are meant to target IP address of computer directly)*
  • Sorry buddy, that’s not my computer, it’s just a router
Defense: Trojans

• Trojans are evil creatures
Defense: Trojans

• Trojans are evil creatures
• Like their namesake (Trojan horse)
  • Seems like a gift, but hidden inside…
• Can be easy to defend against
  • Only use legitimate software (Hint: authentic companies won’t include a Trojan)
  • Avoid “Too Good to Be True”
Defense: Trojan

- Unfortunately, also a bit tricky to find:
  - *Need AV Software & Spyware*
  - *Suspicion is your best friend, first line of defense*

- False positives are a reality
Defense: Spyware

• Spybot Search and Destroy
• Adaware
  • *Free, performs well (last I checked)*

• …Just remember the general defense
• *Cautious of obscure websites*
• *Scan files*
• *Don’t open email files unless expected*
Automation

- Almost mandatory to have automatic:
  - Retrieving/installing program updates
  - Scanning current downloads
  - Scheduled computer scans (nightly – weekly)
  - Scheduled backups (nightly / as-needed)
Obscurity

- Top OS, Browser …safe?

(circa 2013)
Obscurity

• Many Windows users use Outlook/Outlook Express for email client
• About half the world uses Chrome
• Stop and think…

  • *If you were trying to hack a computer system, which one would you target?*
*Passwords*

- Levels of passwords
  - “Throwaway” passwords for sites of no security value
  - More complex passwords for important sites
  - VERY secure password(s) for a very FEW important sites
- Financial sites (banking)
- Main email
- Operating system login
*Passwords*

- A good password:
  - More than seven characters, longer is better
  - Uses letters, numbers, and changes case
  - Not a band, name, or any word
  - Use a song: “Happy Birthday to you”
  - hb2U,hb2U
*Passwords*

- NEVER any reason to share your account, password, or pin
- Administrators, security experts got it, or (most likely) don’t need it
- Don’t be “socially engineered”
- Information is valuable, and dangerous
- Don’t let a sweet-talker get you to say more than you should
Secure Your Network

• Google your router name, find instructions
• Login to router (e.g. http://192.168.0.1)
• Change default password on admin account (usually just “admin”)
• Update firmware
• Good routers are not expensive!
Secure Your Network

• Turn on encryption!
  • *Do not use WEP* (easily cracked)
  • *WPA, WPA-PSK, WPA2*

• Set a password for your wireless network

• Decent network password

• *Wardriving*: searching for open wireless networks to connect to/steal
  • *Programs for this; also lists publicized*
Secure Your Network

• SSID is network name that router broadcasts (visible for those searching)
• Not necessary to disable broadcast
• *Consider changing the name (this alone shows user know-how, scary to hackers)*
  • Dog’s name (e.g. SnoopY)
• Scare others off (e.g. “Riverside Police Lobby”)
• NOT personal information (last name, address)
Secure Your Network

- Advanced Steps (otherwise ignore)
- MAC address filtering: can enable exactly only the computers you want (well, the network cards you want)
- Turning off DHCP, or the automatic assigning of internal addresses → set them yourself

However:
- Friends come over → hassle
Questions?
On Scrap Paper:

1. It’s early, but what do you like/dislike about lecture so far? (Media content, pacing, … anything)

2. Any interesting topics for discussion?