Layered Security
Protecting Your Networked Devices

PCS  SMART PHONES  INTERNET OF THINGS (IOT)
Operating System Firewalls

- Windows Defender Firewall
  - Enabled by default
  - Prompts when a program wants access
- Apple MAC OSX Firewall
  - Not enabled by default
Software Updates

Iterative Software Development Process
- Software is on a constant update cycle
- New features constantly added

Vulnerabilities and Exploits
- Bug Bounties
- Reverse Engineering
Avoidable Attacks – Software Updates

• WannaCry Ransomware Attack
  • Worldwide attack in May 2017
  • A vulnerability known as EternalBlue was exploited
  • A patch to fix EternalBlue was released in February 2017
  • 200,000 computers across 150 countries were infected
Keeping Your System Up-to-Date

Operating System

- Hotfixes/Critical Patches – ASAP
- Patches – Monthly
- Feature Updates – Optional, but recommended
- Version updates – Before EoL

End of Life Operating Systems

- Windows XP – 2014
- Windows 7 – January 2020
- Windows 8.1 – January 2023
- Windows 10 - ? (Rolling Updates)
- MAC OSX 10.13 (High Sierra) and older are no longer supported
Updating Other Applications and Devices

Application Updates

Often automatic
Check “About” or “Help” sections of menus to find updates
Check End-of-Life dates for older applications

Devices – Firmware

Many IoT devices automatically update
Check any app that controls devices for update options
Application Footprints

- Every application installed increases the attack surface
  - Remove unused applications
  - Turn off unnecessary startup applications
  - Only install trusted applications
Malware
Viruses

Parasitic software

- Attaches itself to other content

Infects other programs

- Injects code into other files to make copies of itself

Popular early malware due to the lack of user authentication and access controls
Worms

- Actively seeks out other systems to infect

- Methods of replication:
  - E-mail or IM’s
  - File Sharing
  - Remote execution
  - Remote file access or transfer
  - Remote login
Trojan Horses

- Disguised as a useful or harmless program
- Contains hidden code that, when invoked, delivers a harmful payload
- 3 Models:
  - Functions as expected, but additionally performs malicious activity
  - Modifies the function of the original program to perform malicious activity
  - Only preforms malicious activity and not disguised function
Malware Payloads

- System Corruption
  - Ransomware
  - Data destruction
  - Popups

- Attack Agent
  - Bot/Zombies
  - Botnets

- Information Theft
  - Spyware
  - Keylogger

- Stealthing
  - Backdoor
  - Rootkit
Anti-Virus is a must, even if you have a MAC

Types of Antivirus for PCs

- Simple Scanners – Uses signatures-based detections
- Heuristic Scanners – Uses heuristics to search for probable malware
- Activity traps – Scans memory to identify actions
- Full-feature protection – Uses all the above

Anti-Virus is not full-proof and there are downsides
Extra-Steps to Avoid Malware

• Don’t download e-mail attachments from unknown sources
• Think before you click on a link
• User-Access Control
Personal Computers

- OS Firewalls
  - Protect from incoming attacks
  - Protect unwanted outgoing communications
- Updates
  - Protect from vulnerabilities
  - Fix bugs
  - New Features
- Anti-virus
  - Keep up to date
- Only run trusted applications
- Set up a password and auto lock your computer
Smart Phones

• Updates
  • Protect from vulnerabilities
  • Fix bugs
  • New Features

• Anti-virus
  • Keep up to date

• Only run trusted applications
  • Only use the app store

• Setup up a password/PIN/etc
  • Auto lock your device
IoT Security

- Change default passwords (if possible)
- Turn off any features you don’t need
- Only use approved applications to control
- Update device when possible
- Review permissions of devices and limit when possible