Client and Application Security

> Proper use of machine hardware security systems, securing the operating system, and protecting peripheral devices.

Hardware System Security

Supply Chain Infections are difficult to determine, and revert - it's virtually impossible to monitor every step.

Secure Boot

- BIOS can be updated with malware
- UEFI replaced BIOS to combat attacks, with **secure boot** - checking the signature of the boot sequence

  > BIOS/UEFI → Master Boot Record → Boot Loader → Operating System

Hardware Root of Trust

> Each successive process of the boot sequence relies on the previous for security

Hardware being the root.

- *Shimming* - a middleman between the kernel and driver

Preventing ElecroMagnetic Spying

Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST)

> A classified standard to prevent attackers from picking up ambient readings

Protected Distribution System (PDS)

- *hardened carrier PDS* - special, strengthened electrical tubing
- *alarmed carrier PDS* - fiber optics that sense acoustic vibrations
  - Uses continuous monitoring
  - Carrier can be hidden above the ceiling
  - Eliminates the need to seal connections

Securing Operating Systems

- Network OS - Cisco IOS, Juniper JUNOS, MikroTik, RouterOS
- Server OS - Windows Server, macOS Server, Red Hat

- Workstation OS - Windows, macOS, Ubuntu
- Appliance OS - Linpus Linux
- Kiosk OS - Windows, Chrome, iOS, WebKiosk, KioWare (Android)
- Mobile OS - Android, iOS, Windows Mobile

Security Configuration

- Disable unnecessary ports and services
- Disabling default accounts & passwords
- Employ "least functionality"
- Application whitelisting / blacklisting
- Use tools to automate the configuration process
  - Windows can use "security templates"

  group policy - single configuration to be set and distributed to many / all users.

Patch Management

- security patches repair a discovered vulnerability
- feature updates enhances software, but doesn't address security flaws
- service packs combine both
- automated patch update services manage patches in a local network, rather than using a 3rd party system
  - admins can approve or deny patches, and check to see what hosts can actually use them
- MS forces security updates now

Antimalware

Includes antivirus, antispyware, antispam

Antivirus

- Searches for known patterns in new documents
- Vendor must update and distribute new signature files
- Heuristic Monitoring as a new style - variety of techniques, including code emulation

Antispam

- Basically just a mail gateway
- Whitelists and blacklists
- block certain file types
- Bayesian filtering

Antispyware

- Popup blockers

Trusted OS

- OS hardening, though thorough speculation of code
- Least privilege - remove willy-nilly admin access
- Reduce capabilities - restrict what resources can be accessed
- Read-only filesystems - important OS files can't be changed
- Kernel pruning - remove unnecessary features

Peripheral Security

SD card readers

- Secure Digital Input Output (SDIO) Cards
- Four families - SDSC, SDHC, SDXC, SDIO
- SDIO has wireless transmission built-in via WiFi

Cameras

- three types of speed classes - standard speed, ultra-high speed UHS, video speed
- password-protect the card, use encryption, write-protect the card

External storage

- at-risk to crypto-malware

Multifunction devices

- printer, copier, scanner, fax-machine
- configure to purge stored images
- link to data-loss prevention
- secure-job release for paper-based theft
- use watermarks

Displays

- firmware could be attacked

Physical Security

External perimeter defenses

- barriers, guards, motion detection, rolling barrier, type V controls FIXME
- fencing, cages, bollards
- Barricades are meant to direct traffic flow, not prevent access

Internal physical access security

- door locks, access logs, mantraps, protected cabling distribution systems
  - cipher locks for date/time codes
  - *keyed entry locks* are most common
- Security for protecting hardware devices
- Closed Circuit Television (CCTV)

Application Development Security

Memory Vulnerabilities

- buffer overflow
- DLL injection
- pointer dereferences

Stages

- Development
- Testing
- Staging - "quality assurance"
- Production

  Waterfall vs. Agile

DevOps

- security automation
- continuous integration
- immutable systems
- infrastructure as code
- baselining
- based on agile
- Provisioning - puppet

Methodologies

- model verification
- compiled code testing
- runtime code testing
- static program analyzers
- dynamic analysis (fuzzing)
  - randomized inputs
- stress testing
- integrity measurements