CSF 434/534: Advanced Network and System Security

Week 07 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

Compliance and Frameworks

Compliance and Frameworks

Compliance

- Compliance
  - Meeting the standards of laws, policies, and regulations
- A healthy catalog of rules
  - Across many aspects of business and life
  - Many are industry-specific or situational
- Penalties
  - Fines
  - Incarceration
  - Loss of employment
- Scope
  - Domestic and international requirements

Compliance and Frameworks

Regulatory

- Sarbanes-Oxley Act (SOX)
  - The Public Company Accounting Reform and Investor Protection Act of 2002
- The Health Insurance Portability and Accountability Act (HIPAA)
  - Extensive healthcare standards for storage, use, and transmission of health care information
- The Gramm-Leach-Bliley Act of 1999 (GLBA)
  - Disclosure of privacy information from financial institutions

Compliance and Frameworks

HIPPA Non-compliance penalties

- Extensive fines and penalties
- Ranges for $100 fines to $250,000
- Felony convictions include prison time

Compliance and Frameworks

Non-regulatory

- No rule of law
  - May be strongly suggested
- A regulation may be in the works
  - Get used to the impending change
- Creates value for yourself and/or others
  - You don't need a law if it's the right thing to do
- Sharing of identified malicious IP addresses
  - There's no law or rule that requires you participate
  - It's in your best interest to share

Compliance and Frameworks

Frameworks

- Structure and organization
  - What works best for IT?
- Process management
  - Getting the IT "product" to work best with the organization
- Best practices
  - Guidelines and examples for IT management
  - Cost effective, agile
- Lots of training
  - For everyone

Compliance and Frameworks

Industry-specific frameworks

- COBIT
  - Control Objectives for Information and Related Technologies
  - Created by ISACA, formerly the Information Systems Audit and Control Association
  - Focus on regulatory compliance, risk management and aligning IT strategy with organizational goals
- ITIL
  - Formerly the Information Technology Infrastructure Library
  - Multiple stages of the IT lifecycle
  - Service Design, Service Transition, Service Operation, Service Strategy, Continual Service Improvement

Secure Configuration Guides

Secure Configuration Guides

Secure configurations

- No system is secure with the default configurations
  - You need some guidelines to keep everything safe
- Hardening guides are specific to the software or platform
  - Get feedback from the manufacturer or Internet interest group
  - They'll have the best details
- Other general-purpose guides are available online

Secure Configuration Guides

Web server hardening

- Access a server with your browser
  - The fundamental server on the Internet
  - Microsoft Internet Information Server, Apache HTTP Server, et al.
- Huge potential for access issues
  - Data leaks, server access
- Secure configuration
  - Information leakage: Banner information, directory browsing
  - Permissions: Run from a non-privileged account, configure file permissions
  - Configure SSL: Manage and install certificates
  - Log files: Monitor access and error logs

Secure Configuration Guides

Operating system hardening

- Many and varied
  - Windows, Linux, iOS, Android, et al.
- Updates
  - Operating system updates/service packs, security patches
- User accounts
  - Minimum password lengths and complexity
  - Account limitations
- Network access and security
  - Limit network access
- Monitor and secure
  - Anti-virus, anti-malware

Secure Configuration Guides

Application server

- Programming languages, runtime libraries, etc.
  - Usually between the web server and the database
  - Middleware
- Very specific functionality
  - Disable all unnecessary services
- Operating system updates
  - Security patches
- File permissions and access controls
  - Limit rights to what's required
  - Limit access from other devices

Secure Configuration Guides

Network infrastructure devices

- Switches, routers, firewalls, IPS, etc.
  - You never see them, but they're always there
- Purpose-built devices
  - Embedded OS, limited OS access
- Check with the manufacturer
  - Security updates
  - Not usually updated frequently
  - Updates are usually important

Defense-in-Depth

Defense-in-Depth

Layering the defense

- Physical controls
  - Keep people away from the technology
  - Door locks, fences, rack locks, cameras
- Technical controls
  - Hardware and software to keep things secure
  - Firewalls, active directory authentication, disk encryption
- Administrative controls
  - Policies and procedures
  - Onboarding and off boarding
  - Backup media handling

Defense-in-Depth

Vendor Diversity

- Having multiple suppliers creates vendor diversity, which reduces the risk from any single supplier
- Having only a monoculture raises risks when something specific to that environment fails
- Having two connections to the Internet provides redundancy, and having them operated by separate vendors adds diversity and lowers the risks even more

Control Diversity

- Security controls are the mechanisms by which security functions are achieved
- It is important to have control diversity, both administrative and technical, providing layered security to ensure the controls are effective in producing the desired results
- Total reliance on technical controls without policy provides insufficient security because users who lack policy guidance may utilize a system in ways not foreseen by the implementers of the technical controls, resulting in another risk

Defense-in-Depth

Defense in depth

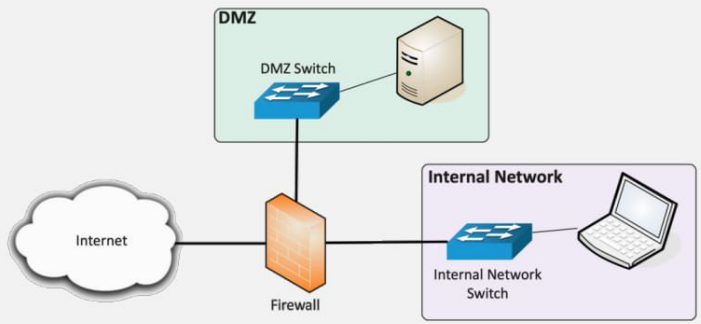
- Firewall
- DMZ
- Hashing passwords
- Authentication
- Anti-virus and anti-malware software
- Intrusion prevention system
- VPN access
- Card/badge access
- Security guard

Secure Network Topologies

Secure Network Topologies

DMZ

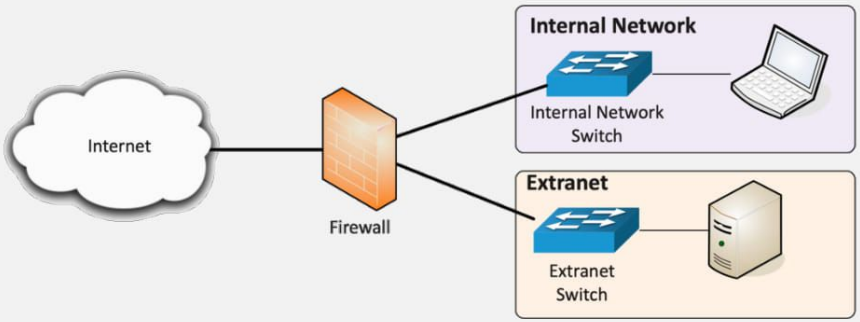
- Demilitarized zone
  - An additional layer of security between the Internet and you
  - Public access to public resources



Secure Network Topologies

Extranet

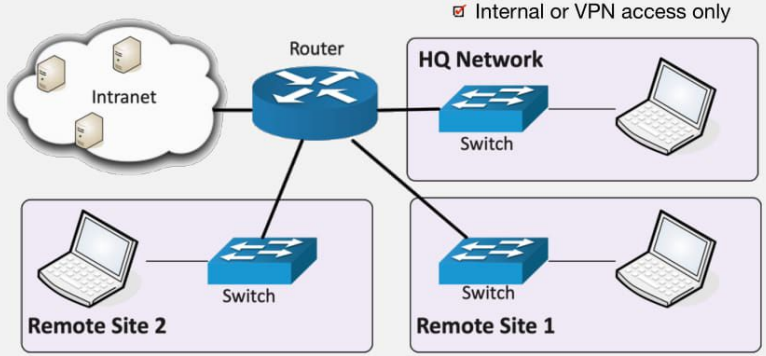
- A private network for partners
  - Vendors, suppliers
- Usually requires additional authentication
  - Only allow access to authorized users



Secure Network Topologies

Intranet

- Private network
  - Only available internally
- Company announcements, important documents, other company business
  - Employees only
- No external access
  - Internal or VPN access only



Secure Network Topologies

Wireless networking

- The convenience of wireless
  - The security concerns of wireless
- Internal use
  - Perhaps configure a separate wireless network for guests
- Users authenticate to the wireless network
  - Use their normal network login credentials
  - 802.1X standard
  - No shared wireless passphrase
  - Integrates into the existing name services

Secure Network Topologies

Ad hoc

- Wireless without an access point
  - Point to point communication
- Common on mobile devices
  - AirDrop, contact sharing apps
- Difficult to control on unmanaged devices
  - Configure ad hoc settings through the MDM
- Implement network access control
  - Use ad hoc, but only with the right credentials
  - Limit application use for ad hoc

Secure Network Topologies

Guest network

- An optional network
  - Convenient for meetings, demonstrations, etc.
- No access to the internal network
  - Internet access only
- Integrate with a captive portal
  - Avoid unauthorized use of the network
  - Useful in congested areas
  - Keeps employees off the guest network

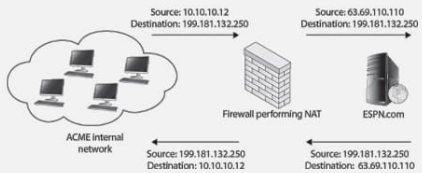
Secure Network Topologies

NAT - Network Address Translation

- It is estimated that there are over 20 billion devices connected to the Internet (and growing)
  - IPv4 supports around 4.29 billion addresses
- The address space for IPv4 is exhausted
  - There are no available addresses to assign
- How does it all work? - Network Address Translation
- This isn't the only use of NAT
  - NAT is handy in many situations

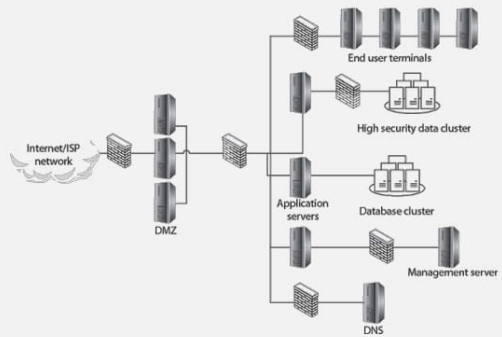
Secure Network Topologies

NAT and security



- NAT is not a security mechanism!
  - There's no protection there
- Security through obscurity
  - The premise: If you can't see it, you can't attack it
  - This isn't security at all
- Bad guys can circumvent an unprotected NAT
  - Sophisticated attacks already assume NAT is in place
  - They will gain access to internal devices, even with NAT
- A stateful firewall is the security mechanism
  - Used in conjunction with NAT to provide security

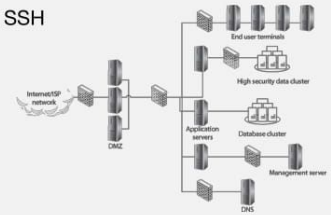
Network Segmentation



Network Segmentation

Segmenting the network

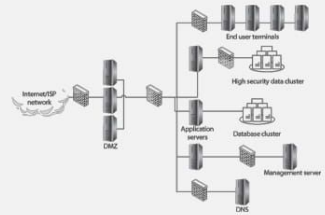
- Physical, logical, or virtual segmentation
  - Devices, VLANs, virtual networks
- Performance
  - High-bandwidth applications
- Security
  - Users should not talk directly to database servers
  - The only applications in the core are SQL and SSH
- Compliance
  - Mandated segmentation (PCI compliance)
  - Makes change control much easier



Network Segmentation

Physical segmentation

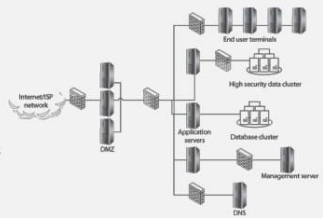
- Devices are physically separate
  - Switch A and Switch B
- Must be connected to provide communication
  - Direct connect, or another switch or router
- Web servers in one rack
  - Database servers on another
- Customer A on one switch, customer B on another
  - No opportunity for mixing data
- Separate devices
  - Multiple units, separate infrastructure



Network Segmentation

Virtualization

- Get rid of physical devices
  - All devices become virtualized
- Servers, switches, routers, firewalls, load balancers
  - All virtual devices
- Instant and complete control
  - Build a new network
  - Route between IP subnets
  - Drop a firewall between
  - Drag and drop devices between networks



Network Segmentation

Air gaps

- One step farther than physical segmentation
  - Physical segmentation usually has some connectivity
- Remove any connectivity between components
  - No possible way for one device to communicate to another
  - No shared components
- Network separation
  - Secure networks
  - Industrial systems (SCADA, manufacturing)
- Some technologies can jump the gap
  - Removable media

Network Segmentation

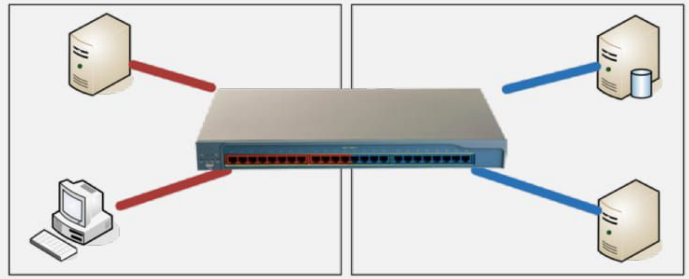
Physical segmentation

- Separate Device
  - Multiple units, separate infrastructure

Network Segmentation

Logical segmentation with VLANs

- Virtual Local Area Networks (VLANs)
  - Separated logically instead of physically
  - Cannot communicate between VLANs without a Layer 3 device / router

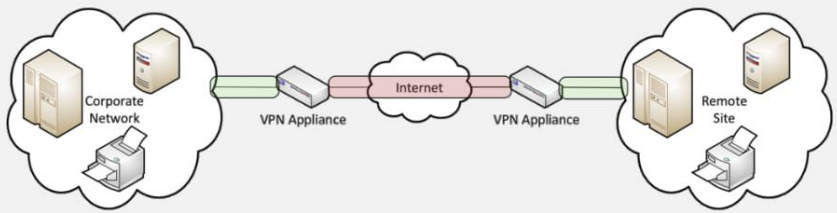


VPN Technologies

VPN Technologies

Site-to-Site VPNs

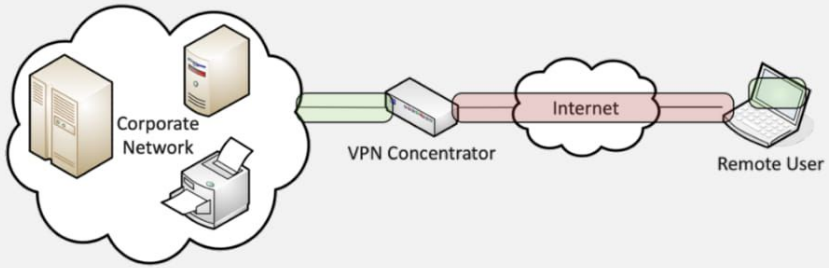
- Encrypt traffic between sites
  - Through the public Internet
- Use existing Internet connection
  - No additional circuits or costs



VPN Technologies

Host-to-Site VPNs

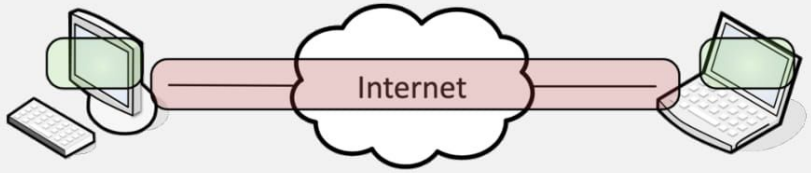
- Also called “remote access VPN”
- Requires software on the user device
  - May be built-in to existing operating system



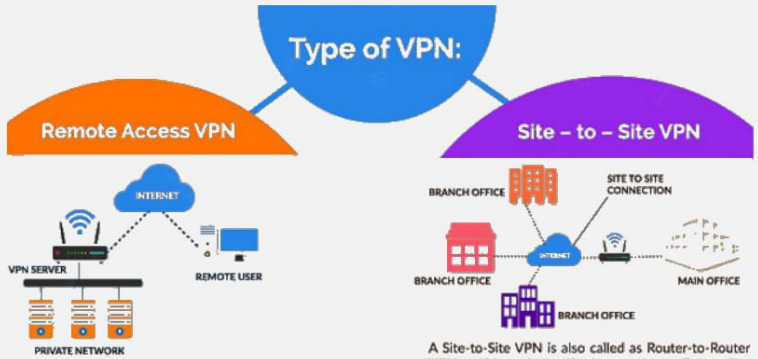
VPN Technologies

Host-to-Host VPNs

- User to user encryption
- Software-based
  - No hardware needed



VPN Technologies



Security Technology Placement

Security Technology Placement

Sensors and collectors

- Gather information from network devices
  - Built-in sensors, separate devices
  - Integrated into switches, routers, servers, firewalls, etc.
- Sensors
  - Intrusion prevention systems, firewall logs, authentication logs, web
  - server access logs, database transaction logs, email logs
- Collectors
  - Proprietary consoles (IPS, firewall), SIEM consoles, syslog servers
  - Many SIEMs include a correlation engine to compare diverse sensor data

Security Technology Placement

Filters and firewalls

- Packet filters
  - Simple data blocks - ignores state
  - Linux iptables - filter packets in the kernel
  - Usually placed on a device or server
- Firewalls
  - State-based
  - Advanced filtering by IP address, port, application, content
  - Usually located on the ingress/egress of a network
  - Some organizations place them between internal networks

Security Technology Placement

Proxy servers

- An intermediate server
  - Client makes the request to the proxy
  - The proxy performs the actual request
  - The proxy provides results back to the client
- Useful features
  - Access control, caching, URL filtering, content scanning

Security Technology Placement

Forward proxy

- Protect users from the Internet

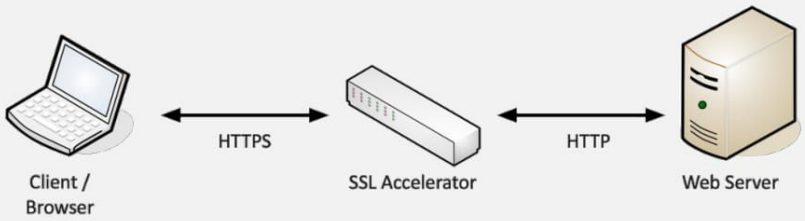
VPN concentrators

- VPN appliances are usually located on the edge of the network
  - Internet-facing
- Sites connect from one site to another across the Internet

Security Technology Placement

SSL accelerators

- The SSL handshake requires some cryptographic overhead
  - A lot of CPU cycles
- Offload the SSL process to a hardware accelerator
  - Often integrated into a load balancer



Security Technology Placement

Load balancers

- Manage the load across multiple devices
  - The user has no idea
  - Placed between the users and the service
- Servers can be added and removed
  - Real-time response to load
- Load balancer performs constant health checks
  - If a server disappears, it is removed from the rotation

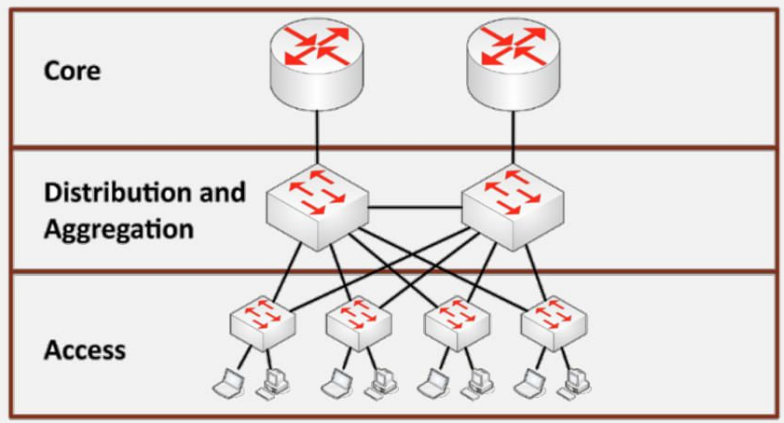
Security Technology Placement

DDoS mitigation

- Resist a distributed denial of service attack
  - Minimize the impact
- Cloud-based
  - Internet provider or reverse proxy service
- On-site tools
  - DDoS filtering in a firewall or IPS
- Positioned between you and the Internet
  - Literally you against the world

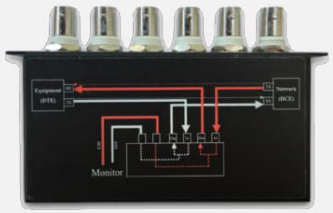
Security Technology Placement

Aggregation switches



Security Technology Placement

Taps and port mirrors



- Intercept network traffic
  - Send a copy to a packet capture device
- Physical taps
  - Disconnect the link, put a tap in the middle
  - Can be an active or passive tap
- Port mirror
  - Port redirection, SPAN (Switched Port Analyzer)
  - Software-based tap
  - Limited functionality, but can work well in a pinch

Securing SDN

Software Defined Networking

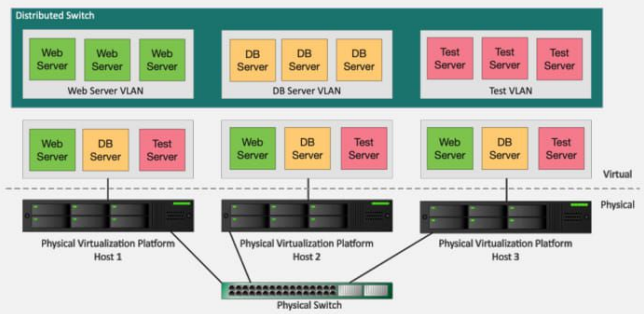
SDN (Software Defined Networking)

- Networking devices have two functional planes of operation
  - Control plane
  - Data plane
- Directly programmable
  - Configuration is different than forwarding
- Agile
  - Changes can be made dynamically
- Centrally managed - Global view, single pane of glass
- Programmatically configured
  - Orchestration - No human intervention
- Open standards / vendor neutral
  - A standard interface to the network

Software Defined Networking

Distributed switching

- Remove the physical segmentation
  - A virtual network distributed across all physical platforms
- When a VM moves, the network doesn't change
  - Servers will always connect to the right VLAN



Hardware Security

Hardware Security

Full Disk Encryption (FDE) / Self-Encrypting Drive (SED)

- Encrypt an entire drive
  - Not just a single file
- Protects all of your data
  - As well as the operating system
- Lose you laptop?
  - Doesn't matter without the password
- Data is always protected
  - Even if the physical drive is moved to another computer
- Built-in to the operating system
  - Microsoft BitLocker, Apple FileVault, Linux Unified Key Setup (LUKS)

Hardware Security

Trusted Platform Module (TPM)

- A specification for cryptographic functions
  - Hardware to help with all of this encryption stuff
- Cryptographic processor
  - Random number generator, key generators
- Persistent memory
  - Comes with unique keys burned in during production
- Versatile memory
  - Storage keys, hardware configuration information
- Password protected
  - No dictionary attacks

Hardware Security

Hardware Security Module (HSM)

- High-end cryptographic hardware
  - Plug-in card or separate hardware device
- Key backup
  - Secured storage
- Cryptographic accelerators
  - Offload that CPU overhead from other devices
- Used in large environments
  - Clusters, redundant power

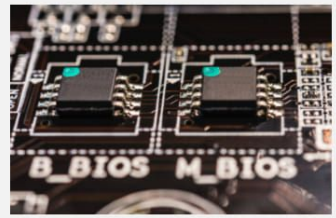
Hardware Security

Hardware root of trust

- Security is based on trust
  - Is your data safely encrypted?
  - Is this web site legitimate?
- The trust has to start somewhere
  - TPM, HSM
  - Designed to be the hardware root of the trust
- Difficult to change or avoid
  - It's hardware
  - Won't work without the hardware

Hardware Security

UEFI BIOS



- Unified Extensible Firmware Interface
  - Based on Intel's EFI (Extensible Firmware Interface)
- A defined standard
  - Implemented by the manufacturers
- Designed to replace the legacy BIOS
  - Need a modern BIOS for modern computers

Hardware Security

Secure Boot

- Malicious software can "own" your system
  - Malicious drivers or OS software
- Secure boot
  - Part of the UEFI specification
- Digitally sign known-good software
  - Cryptographically secure
  - Software won't run without the proper signature
- Support in many different operating systems
  - Windows, Linux Fedora, openSUSE, Ubuntu
  - Apple uses their own EFI implementation

Hardware Security

Remote attestation

- Nothing on this computer has changed
  - There have been no malware infections
  - How do you know?
- Easy when it's just your computer
  - More difficult when there are 1,000
- Remote attestation
  - Device provides an operational report to a verification server
  - Encrypted and digitally signed with the TPM
  - Changes are identified and managed

Hardware Security

Supply chain

- September 2015: Hundreds of Cisco routers infected with “SYNful Knock”
  - Firmware modified for back-door access
- Can you trust your new server/router/switch/firewall?
  - Supply chain cyber security
- Use trusted vendors
- Critical devices should not be connected to the outside
- Verify your hardware is genuine

Hardware Security

EMI/EMP

- Electromagnetic interference /Electromagnetic pulse
- EMI leakage
  - Determine data streams based on EMI emissions
  - Keyboards, hard drives, network connections
- Modify the security by injecting EMI
  - Change sensor data and other input
- Shielding against EMP
  - Important for national security and infrastructure

Operating System Security

Operating System Security

Operating system types

- There’s a little overlap in most operating systems
- Network
  - Supports servers, workstations, and other network-connected devices
- Server
  - Designed to operate as a server
  - Web server, database server
- Workstation
  - Optimized for user applications
  - Email, browsing, office apps, video editing

Operating System Security

Operating system types (cont.)

- Appliance
  - Purpose-built
  - Usually a minimal OS, often unseen by the user
- Kiosk
  - Public device
  - OS is tightly locked down
- Mobile OS
  - Designed for touch screen phones and tablets
  - Optimized for mobile hardware

Operating System Security

Patch management

- Incredibly important
  - System stability, security fixes
- Service packs
  - All at once
- Monthly updates - Incremental (and important)
- Emergency out-of-band updates
  - Zero-day and important security discoveries

Operating System Security

Update options

- Windows update
  - Bring Windows up-to-date on each workstation
- Windows Server Update Services (WSUS)
  - Centralized management for Windows devices
- Mac OS
  - Software Update
  - Available on the Apple menu
- Linux - Many different options
  - yum, atp-get, rpm, graphical front-ends

Operating System Security

The patching process

- Not always seamless
  - May take some planning
- May introduce other problems
  - The fix can cause another problem
- Pick and choose
  - You don't have to install every single patch
- Often centrally managed
  - The update server determine when you patch
  - Test all of your apps, then deploy
  - Efficiently manage bandwidth

Operating System Security

Disabling unnecessary services

- "Unnecessary" isn't always obvious
  - Windows XP included almost 90 services by default, Windows 7 has over 130
- Every service has the potential for trouble
  - The worst vulnerabilities are 0-day
- This may require a lot of research
  - Many different sources
  - Don't rely on the manufacturer
- Trial and error may be necessary
  - Testing and monitoring

Operating System Security

Least functionality

- Limit the operating system to only what's needed
  - Every function has a potential security risk
- May be different depending on the use
  - Shipping / receiving vs. IT development vs. a kiosk
- Extensive configurations
  - Disable printer installation
  - Disable changing system time
  - Disable taking ownership of file system objects
  - Deny log on as a service

Operating System Security

Secure configurations

- Fine tuning of the operating system
  - Make your least functionality very secure
- These will apply regardless of the system use
  - The operating system is common to all
- Example secure configuration policies
  - Stay updated with the latest patches
  - Compromised systems are re-imaged (not "cleaned")
  - Changes to the standard build must go through change management
  - Perform regular integrity checks of operating system files

Operating System Security

Evaluation Assurance Level

- Common Criteria for Information Technology Security Evaluation
  - Also called Common Criteria (or CC)
  - An international computer security certification standard (ISO/IEC 15408)
  - A common reference for US Federal Government
- Evaluation Assurance Level (EAL)
  - EAL1 through EAL7
- Trusted operating system
  - The operating system is EAL compliant
  - EAL4 is the most accepted minimum level

Operating System Security

Application whitelisting/blacklisting

- Any application can be dangerous
  - Vulnerabilities, trojan horses, malware
- Security policy can control app execution
  - Whitelisting and blacklisting
- Whitelisting
  - Nothing runs unless it's approved
  - Very restrictive
- Blacklisting
  - Nothing on the "bad list" can be executed
  - Anti-virus, anti-malware

Operating System Security

Examples of application management

- Decisions are made in the operating system
  - Often built-in to the operating system management
- Application hash
  - Only allows applications with this unique identifier
- Certificate
  - Allow digitally signed apps from certain publishers
- Path
  - Only run applications in these folders
- Network zone
  - The apps can only run from this network zone

Operating System Security

Disabling unnecessary accounts

- All operating systems include other accounts
  - guest, root, mail, etc.
- Not all accounts are necessary
  - Disable/remove the unnecessary
- Disable interactive logins
  - Not all accounts need to login

Peripheral Security

Operating System Security

Wireless keyboards and mice

- Many wireless keyboards and mice communicate in the clear
  - Use proprietary wireless communication protocols
  - Over 2.4 GHz frequencies
- Easy to capture keystrokes with a receiver
  - Inject keystrokes and mouse movements
  - Control the computer remotely
  - Vulnerability called “KeySniffer”
- Some keyboard manufacturers support AES encryption

Operating System Security

Displays

- Electromagnetic radiation
  - View information on a screen by eavesdropping the EM signals
  - Internal signals of a laptop or external cable
  - Eavesdrop through the walls
- Firmware hacks
  - Many displays have no security for firmware upgrades
  - Log information on the screen
  - Ransomware with an LCD display

Operating System Security

WiFi-enabled microSD

- Combination SD flash storage device and 802.11 Wi-Fi file transfers
  - Transfer from a camera to a computer without removing the SD card
- SD card authentication vulnerabilities
  - Predictable access, easy to read files over Wi-Fi
- API access to the SD card
  - Manufacturer must implement strong security
  - API access can result in data leakage or data loss

Operating System Security

Printers/multi-function devices

- Multi-function devices
  - Printer, scanner, fax
  - Network connectivity
  - Local storage
- Reconnaissance
  - Log files for all activity, address books
- Unauthorized access
  - Print without authentication
  - Capture spool files

Operating System Security

External storage devices

- Storage outside the computer, and often removable
  - Very portable, easy to move large files
- No authentication
  - Anyone can connect and read
  - Always use file/volume encryption
- Often used for exfiltration of data
  - Manage the use of removal storage

Operating System Security

Digital cameras

- Capture still images and video
  - Save to digital storage
- Device operates as external storage
  - Easy to move data around
- Camera firmware can be compromised
  - Security cameras are also vulnerable

Secure Deployments

Secure Deployments

Development to production

- Your programming team has been working on a new application
  - How will you deploy it safely and reliably?
- Patch Tuesday
  - Test and deploy Wednesday? Thursday? Friday?
- Manage the process
  - Safely move from a non-production phase to full production

Secure Deployments

Sandboxing

- Isolated testing environment
  - No connection to the real world or production system
  - A technological safe space
- Use during the development process
  - Try some code, break some code, nobody gets hurt
- Incremental development
  - Helps build the application

Secure Deployments

Working environments

- Development
  - Secure environment
  - Writing code
  - Developers test in their sandboxes
- Test - Still in the development stage
  - All of the pieces are put together
  - Does it all work?
  - Functional tests, quality assurance (QA) testing
  - If it works in test, then it's ready for staging

Secure Deployments

Working environments (cont.)

- Staging - Almost ready to roll it out
  - Works and feels exactly like the production environment
  - Working with a copy of production data
  - Run performance tests
  - Test usability and features
- Production - Application is live
  - Rolled out to the user community

Secure Deployments

Secure baselines

- The security of an application environment should be well defined
  - All application instances must follow this baseline
  - Firewall settings, patch levels, OS file versions
  - May require constant updates
- Integrity measurements check for the secure baseline
  - These should be performed often
  - Check against well-documented baselines
  - Failure requires an immediate correction

Embedded Systems

Embedded Systems

SCADA/ICS

- Supervisory Control and Data Acquisition System
  - Large-scale, multi-site Industrial Control Systems (ICS)
- PC manages equipment
  - Power generation, refining, manufacturing equipment
- Distributed control systems
  - Real-time information
  - System control
- Requires extensive segmentation
  - No access from the outside

Embedded Systems

Smart devices/IoT (Internet of Things)

- Wearable technology
  - Glasses, watches, health monitors
  - Early generation products
  - Track our location
  - Where is that data and how is it stored?
- Home automation
  - Video doorbells
  - Internet-connected garage door openers
  - Heating and cooling
  - It knows when you are home (and when you aren't)

Embedded Systems

HVAC

- Heating, Ventilating, and Air Conditioning
  - Thermodynamics, fluid mechanics, and heat transfer
- A complex science
  - Not something you can properly design yourself
  - Must be integrated into the fire system
- PC manages equipment
  - Makes cooling and heating decisions for workspaces and data centers
- Traditionally not built with security in mind
  - Difficult to recover from an infrastructure DoS

Embedded Systems

SoC (System on a Chip)

- Multiple components running on a single chip
  - Common with embedded systems
- Small form-factor
  - External interface support
  - Cache memory, flash memory
  - Usually lower power consumption
- Security considerations are important
  - Difficult to upgrade hardware
  - Limited off-the-shelf security options

Embedded Systems

RTOS (Real-Time Operating System)

- An operating system with a deterministic processing schedule
  - No time to wait for other processes
  - Industrial equipment, automobiles,
  - Military environments
- Extremely sensitive to security issues
  - Non-trivial systems
  - Need to always be available
  - Difficult to know what type of security is in place

Embedded Systems

Printers, scanners, and fax machines

- All-in-one or multifunction devices (MFD)
  - Everything you need in one single device
- No longer a simple printer
  - Very sophisticated firmware
- Some images are stored locally on the device
  - Can be retrieved externally
- Logs are stored on the device
  - Contain communication and fax details

Embedded Systems

Camera systems

- Video monitoring for home or office
  - 24 hour / 7 day video (and audio)
- Video recorders are IP devices
  - Authenticate using a specialized application
- Cameras are IP devices
  - 4K/high definition
- Privacy concerns
  - Don't need to ring a doorbell
  - We know when you are home
  - We might even see you

Embedded Systems

Special purpose

- Medical devices
  - Heart monitors, insulin pumps
  - Often use older operating systems
- Vehicles
  - Internal network is often accessible from mobile networks
  - Control internal electronics
  - Disable the engine
- Aircraft/UAV (Unmanned aerial vehicle)
  - DoS could damage the aircraft and others on the ground

CSF 434/534: Advanced Network and System Security

Week 07 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes