CSF 434/534: Advanced Network and System Security

Week 06 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

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

Command Line Security Tools

Command Line Security Tools

ping

- Test reachability
  - Determine round-trip time
  - Uses Internet Control Message Protocol (ICMP)
- One of your primary troubleshooting tools
  - Can you ping the host?
- Written by Mike Muuss in 1983
  - The sound made by sonar
  - Not an acronym for Packet INternet Groper
  - A backronym

Command Line Security Tools

netstat

- Network statistics
  - Many different operating systems

netstat -a

- Show all active connections

netstat -b

- Show binaries

netstat -n

- Do not resolve names

Command Line Security Tools

traceroute

- Determine the route a packet takes to a destination
  - Map the entire path

***tracert* (Windows) or *traceroute* (POSIX)**

- Takes advantage of ICMP Time to Live Exceeded error message
  - The time in TTL refers to hops, not seconds or minutes
  - TTL=1 is the first router, TTL=2 is the second router, etc.
- Not all devices will reply with ICMP Time Exceeded messages
  - Some firewalls filter ICMP
  - ICMP is low-priority for many devices

Command Line Security Tools

nslookup and dig

- Lookup information from DNS servers
  - Canonical names, IP addresses, cache timers, etc.

nslookup

- Both Windows and POSIX-based
  - Lookup names and IP addresses
  - Deprecated (use dig instead)

***dig* or DiG (Domain Information Groper)**

- More advanced domain information
  - Probably your first choice
  - Windows: http://www.isc.org/downloads/bind/

Command Line Security Tools

Address Resolution Protocol

- Determine a MAC address based on an IP address
  - You need the hardware address to communicate
- *arp -a*
  - View local ARP table

ipconfig* and *ifconfig

- Most of your troubleshooting starts with your IP address
  - Ping your local router/gateway
- Determine TCP/IP and network adapter information
  - And some additional IP details
- *ipconfig* – Windows TCP/IP configuration
- *ifconfig* – Linux interface configuration

Command Line Security Tools

tcpdump

- Capture packets from the command line
  - Very convenient
- Available in most Unix/Linux operating systems
  - Included with Mac OS X, available for Windows (WinDump)
- Apply filters, view in real-time
  - Quickly identify traffic patterns
- Save the data, use in another application
  - Written in standard pcap format
- Can be an overwhelming amount of data
  - Takes a bit of practice to parse and filter

Command Line Security Tools

Nmap

- Network mapper
  - Find and learn more about network devices
- Port scan
  - Find devices and identify open ports
- Operating system scan
  - Discover the OS without logging in to a device
- Service scan
  - What service is available on a device? Name, version, details
- Additional scripts
  - Nmap Scripting Engine (NSE)
    - Extend capabilities, vulnerability scans

Command Line Security Tools

netcat

- "Read" or "write" to the network
  - Open a port and send or receive some traffic
- Many different functions
  - Listen on a port number
  - Transfer data
  - Scan ports and send data to a port
- Become a backdoor
  - Run a shell from a remote device
- Other alternatives and OSes - Ncat

Common Security Issues

Common Security Issues

Unencrypted credentials

- Authentication is a critical process
  - All data must be protected
- Some protocols aren't encrypted
  - All traffic sent in the clear
  - Telnet, FTP, SMTP, IMAP
- Verify with a packet capture
  - View everything sent over the network

Common Security Issues

Logs and event anomalies

- Gather as much information as possible
  - Will be important later
- Many different sources
  - Switches, routers, firewalls, servers, IPS
- Use a security information and event management (SIEM) system
  - Consolidate logs and correlate data
  - Extensive reporting

Common Security Issues

Permission issues

- A simple oversight
  - A huge vulnerability
  - The door was left open - no lockpicking required
- June 2017 - 14 million Verizon records exposed
  - Third-party left an Amazon S3 data repository open
  - Researcher found the data before the bad guys
- Confirm permissions on initial configuration
  - Provide a process for changes and updates
  - Perform periodic audits

Common Security Issues

Access violations

- Segmentation fault
- Your operating system is looking out for you
  - Prevents access to a restricted area of memory
- Might be a programming error
  - A pointer to the wrong location
- Could be a security issue
  - Malware attempting to access restricted memory
  - Denial of service

Common Security Issues

Certificate issues

- A certificate should be signed by someone you trust
  - It's really someone your computer trusts
- Certificates should also be relatively new
  - You don't want certificates to get too old
- Application must perform the proper certificate checks
- February 2017 - Researcher finds seventy-six iOS apps that are missing TLS certificate checks
  - 18 million downloads - Easy to MitM attack

Common Security Issues

Data exfiltration

- Data is your most valuable asset
  - It might also be valuable to other people
- You've built a high-speed network
  - Also easy to remove through DVD-ROMs or USB flash drives
- July 2017 - Time Warner / Home Box Office
  - 1.5 terabytes of data exfiltrated
  - "HBO recently experienced a cyber incident, which resulted in the compromise of proprietary information."

Common Security Issues

Misconfigured devices

- Another example of leaving the door open
  - The bad guys walk right in
- Default username and password - Easy to authenticate
- Outdated software - Known vulnerabilities
- Running maintenance code
  - Debug information displayed to users

Common Security Issues

Misconfigured devices (cont.)

- Firewalls
  - Rules provide too much access
  - Can be difficult to audit with a large rule base
- Content filters
  - URLs are not specific enough
  - Some protocols not filtered (i.e., https)
- Access points
  - No encryption mechanisms
  - Open configurations from the wireless side

Common Security Issues

Weak security configurations

- Digital security works great
  - Until it doesn't work great any longer
- Too old - DES (Data Encryption Standard) encryption
  - Created in 1975, 56 bit keys
  - Small key size is easily brute-forced with today's technologies
- Encryption vulnerabilities - WEP (Wired Equivalent Privacy)
  - Initial 802.11 encryption algorithm
  - Vulnerabilities found with RC4 ciphers and IVs
- Hash collisions - SHA-1 (Secure Hash Algorithm 1)
  - Many collision attacks identified - Different documents with the same hash - No longer viable

Common Security Issues

Personnel issues

- The weakest link - People make mistakes
- Policy violations
  - It's in your Acceptable Use Policy (AUP) document
- Insider threats
  - Authenticated users have more free reign than non-authenticated
  - Important to assign the correct rights and permissions

Common Security Issues

Personnel issues (cont.)

- Social engineering
  - We're always so willing to help someone in need
  - They'll steal everything over the phone
- Social media
  - Posting of internal information
  - Public companies must not disclose meaningful information
  - Most organizations have a policy and marketing team
- Personal emails
  - Emails sent from work imply endorsement by the organization
  - Uses company resources

Common Security Issues

Unauthorized software

- You don't know where that's been
  - Malware, spyware, ransomware
- Conflicts
  - May conflict with the organization's software
- Licensing
  - You're going to pay for that, right?
- Ongoing support
  - Who's going to upgrade the unauthorized software? Security patches?
  - What happens when it stops working?

Common Security Issues

Baseline deviation

- Everything should be well documented
  - Hardware, software, network traffic patterns, data storage
- Any changes to the norm should be identified
  - And alerts should be sent immediately
- Common with VPNs
  - Security posture analysis before connecting to the network
  - If something deviates from the baseline, you must fix it
    - Anti-virus and signature version, OS patches
  - No remote access until it matches the baseline

Common Security Issues

License compliance violation

- So many software licenses
  - Operating systems, applications, hardware appliances
  - And they all license with different methodologies
- Availability
  - Everything works great when the license is valid
  - Meeting the expiration date may cause problems
  - Application may stop working completely
- Integrity
  - Data and applications must be accurate and complete
  - A missing/bad license may cause problems with data integrity

Common Security Issues

Asset management

- Identify and track computing assets
  - Usually an automated process
- Respond faster to security problem
  - You know who, what, and where
- Keep an eye on the most valuable assets
  - Both hardware and data
- Track licenses
  - You know exactly how many you'll need
- Verify that all devices are up to date
  - Security patches, anti-malware signature updates, etc.

Common Security Issues

Authentication issues

- Is someone really who they say they are?
- Number of factors
  - The more, the better
  - The more, the more chance of problems
- A lapse in any part of the authentication process can open the entire network
  - Weak passwords, not enough authentication factors, etc.

Analyzing Security Output

Analyzing Security Output

Host-based IDS/IPS

- Intrusion Detection System / Intrusion Prevention System
- Started as a separate application
  - Now integrated into many “endpoint” products
- Protect based on signatures
  - Decrypted data
- Protect based on activity
  - Why are you modifying that file?

Analyzing Security Output

Antivirus

- The viruses are out there
  - It’s just a matter of time
- From computers running Kaspersky Lab products in Q1 2017:
  - 479,528,279 malicious attacks blocked
  - 79,209,775 malicious URLs identified
  - 240,799 blocked ransomware attacks
  - 1,333,605 malicious installation packages on mobile devices
  - http://professormesser.link/q1stats
- Antivirus apps will alert and log on malicious software
  - Download or execute
  - Visit known-bad URL

Analyzing Security Output

File integrity check

- Operating system check
  - Are the original files still in place?
- Host based firewalls
- Protect against others on the network
  - Restrict access to your personal computer
- Protect wherever you go
  - Required for laptops and mobile devices
- Restricts by application and network port numbers
  - The firewall knows what you’re doing
- Log displays connection attempts
  - Allowed and denied access

Analyzing Security Output

Application whitelisting

- 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

Analyzing Security Output

Removable media control

- USB drives, portable hard drives
  - The bane of the security professional
- Malware infections
  - Drives brought from home
  - USB drives all over the parking lot
- Exfiltration - Terabytes of data that fits into your pocket
- Windows Event Log
  - Security auditing
  - View USB media use, log filenames copied to removable drives

Analyzing Security Output

Advanced malware tools

- Specialized removal and recovery tools
  - Malware techniques vary widely
- Malware is pervasive
  - Spreads to all parts of your operating system
- The best recovery is to delete and restore from good backup
  - You don't always have this option
- Research as much as possible
  - Gather recon from the malware tools
  - Stop it and prevent it

Analyzing Security Output

UTM/All-in-one security appliance

- Unified Threat Management (UTM) / Web security gateway
  - URL filter / Content inspection
  - Malware inspection
  - Spam filter
  - CSU/DSU
  - Router / Switch
  - Firewall
  - IDS/IPS
  - Bandwidth shaper
  - VPN endpoint

Analyzing Security Output

Data Loss Prevention (DLP)

- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Stop the data before the bad guys get it
  - Data "leakage"
- So many sources, so many destinations
  - Often requires multiple solutions in different places

Analyzing Security Output

Data Execution Prevention (DEP)

- No-eXecute bit
  - Intel calls it the XD bit (eXecute Disable)
  - AMD calls it Enhanced Virus Protection
- Designate sections of memory as executing code or data
  - Code can't run from protected memory locations
  - Prevents malware and viruses from executing
- The OS must support this feature
  - Windows calls it Data Execution Prevention (DEP)
  - Enabled automatically as a default
  - All logs are in the Event Viewer

Analyzing Security Output

Web application firewall (WAF)

- Not like a "normal" firewall
  - Applies rules to HTTP conversations
- Allow or deny based on expected input
  - Unexpected input is a common method of exploiting an application
- SQL injection
  - Add your own commands to an application's SQL query
- A major focus of Payment Card Industry Data Security Standard (PCI DSS)

Mobile Device Connection Methods

Mobile Device Connection Methods

Cellular networks

- Mobile devices
  - "Cell" phones
- Separate land into "cells"
  - Antenna coverages a cell with certain frequencies
- Security concerns
  - Traffic monitoring
  - Location tracking
  - Worldwide access to a mobile device

Mobile Device Connection Methods

Wi-Fi

- Local network access
  - Local security problems
- Same security concerns as other Wi-Fi devices
- Data capture
  - Encrypt your data!
- Man-in-the-middle
  - Modify and/or monitor data
- Denial of service
  - Frequency interference

Mobile Device Connection Methods

Satellite communications - SATCOM

- Remote locations, natural disasters
  - Standard communication won't work
- Literally talking to space
  - Satellites in a low earth orbit or geostationary
- Voice and data communication
  - Communicate from almost anywhere
- Handheld devices can be a security risk
  - Operating system vulnerabilities
  - Remote code execution
  - Similar security issues to other smartphones

Mobile Device Connection Methods

Near field communication (NFC)

- Two-way wireless communication
  - Builds on RFID, which was one-way
- Payment systems
  - Google wallet and MasterCard partnership
  - Apple Pay
- Bootstrap for other wireless
  - NFC helps with Bluetooth pairing
- Access token, identity "card"
  - Short range with encryption support

Mobile Device Connection Methods

NFC security concerns

- Remote capture
  - It's a wireless network
  - 10 meters for active devices
- Frequency jamming
  - Denial of service
- Relay / Replay attack
  - Man in the middle
- Loss of RFC device control
  - Stolen/lost phone

Mobile Device Connection Methods

ANT/ANT+

- Wireless sensor network protocol
  - 2.4 GHz ISM band (industrial, scientific, and medical)
  - An “Internet of Things” ultra-low-power protocol
  - Fitness devices, heart rate monitors, etc.
- A separate wireless service
  - Not 802.11 or Bluetooth
- Denial of service
  - Spectrum jamming
- Optional encryption
  - And no method to maintain integrity

Mobile Device Connection Methods

IR (Infrared)

- Included on many smartphones, tablets, and smartwatches
  - Not really used much for file transfers and printing
- Control your entertainment center
  - Almost exclusively IR
- File transfers are possible
- Other phones can be used to control your IR devices

Mobile Device Connection Methods

USB (Universal Serial Bus)

- Physical connectivity to your mobile device
  - USB to your computer
  - USB, Lightning, or proprietary on your phone
- Physical access is always a concern
  - May be easier to gain access than over a remote connection
- A locked device is relatively secure
  - Always auto-lock
- Mobile phones can also exfiltrate
  - Phone can appear to be a USB storage device

Connection Methods

- If you find a USB thumb drive on the ground in a parking lot, do not attach it to a machine and report it to security as soon as possible

- Doesn’t need to look like a threat to be a threat

Mobile Device Management

Mobile Device Management

Mobile Device Management (MDM)

- Manage company-owned and user-owned mobile devices
  - BYOD - Bring Your Own Device
- Centralized management of the mobile devices
  - Specialized functionality
- Set policies on apps, data, camera, etc.
  - Control the entire remote device or a “partition”
- Manage access control
  - Force screen locks and PINs on these single user devices

Mobile Device Management

Application management

- Managing mobile apps are a challenge
  - Mobile devices install apps constantly
- Not all applications are secure
  - And some are malicious
  - Android malware is a growing security concern
- Manage application use through whitelists
  - Only approved applications can be installed
  - Managed through the MDM
  - New applications must be checked and added

Mobile Device Management

Content management

- Mobile Content Management (MCM)
  - Secure access to data
  - Protect data from outsiders
- File sharing and viewing
  - On-site content (Microsoft Sharepoint, file servers)
  - Cloud-based storage (Box, Office 365)
- Data sent from the mobile device
  - DLP (Data Loss Prevention) prevents copy/paste of sensitive data
  - Ensure data is encrypted on the mobile device
- Managed from the mobile device manager (MDM)

Mobile Device Management

Remote wipe

- Remove all data from your mobile device
  - Even if you have no idea where it is
  - Often managed from the MDM
- Connect and wipe from the web
  - Nuke it from anywhere
- Need to plan for this
  - Configure your mobile device now
- Always have a backup
  - Your data can be removed at any time
  - As you are walking out the door

Mobile Device Management

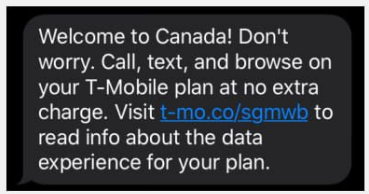
Geolocation

- Precise tracking details
  - Tracks within feet
- Can be used for good (or bad)
  - Find your phone
  - Find you
- Most phones provide an option to disable
  - Limits functionality of the phones
- May be managed by the MDM

Mobile Device Management

Geofencing

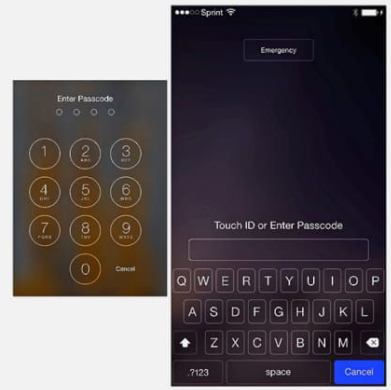
- Some MDMs allow for geofencing
  - Restrict or allow features when the device is in a particular area
- Cameras
  - The camera might only work when outside the office
- Authentication
  - Only allow logins when the device is located in a particular area



Mobile Device Management

Screen lock

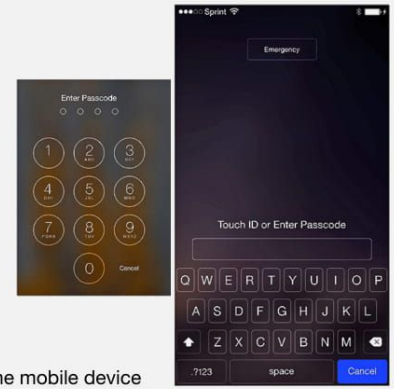
- All mobile devices can be locked
  - Keep people out of your data
- Simple passcode or strong passcode
  - Numbers vs. Alphanumeric
- Fail too many times?
  - Erase the phone
- Define a lockout policy
  - Create aggressive lockout timers
  - Completely lock the phone



Mobile Device Management

Passwords and PINs

- The universal help desk call
  - I need to reset my password
- Mobile devices use multiple authentication methods
  - Password/passphrase, PINs, patterns
- Recovery process can be initiated from the MDM
  - Password reset option is provided on the mobile device
- MDM also has full control
  - Completely remove all security controls
  - Not the default or best practice



- You should always consider password complexity
- 4 digit passcode = 10^4 possible permutations
- Length is better than ComPl3x!7y ~ but you should have a strong mix of both

Mobile Device Management

Biometrics

- You are the authentication factor
  - Fingerprint, face
- May not be the most secure authentication factor
  - Useful in some environments
  - Completely forbidden in others
- Availability is managed through the MDM
  - Organization determines the security of the device
- Can be managed per-app
  - Some apps require additional biometric authentication

Mobile Device Management

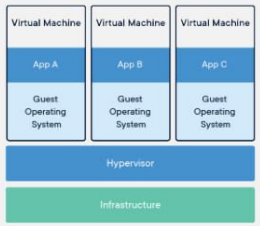
Context-aware authentication

- Who needs 2FA?
  - The bad guys can get around anything
- Authentication can be contextual
  - If it walks like a duck...
- Combine multiple contexts
  - Where you normally login (IP address)
  - Where you normally frequent (GPS information)
  - Other devices that may be paired (Bluetooth, etc.)
  - And others
- An emerging technology
  - Another way to keep data safe

Mobile Device Management

Containerization

- Difficult to separate personal from business
  - Especially when the device is BYOD
  - Owned by the employee
- Separate enterprise mobile apps and data
  - Create a virtual “container” for company data
  - A contained area - limit data sharing
  - Storage segmentation keeps data separate
- Easy to manage offboarding
  - Only the company information is deleted
  - Personal data is retained
  - Keep your pictures, video, music, email, etc.



Mobile Device Management

Full device encryption

- Scramble all of the data on the mobile device
  - Even if you lose it, the contents are safe
- Devices handle this in different ways
  - Strongest/stronger/strong ?
- Encryption isn't trivial
  - Uses a lot of CPU cycles
  - Complex integration between hardware and software
- Don't lose or forget your password!
  - There's no recovery

Mobile Device Enforcement

Mobile Device Enforcement

Third-party app stores

- Centralized app clearinghouses
  - Apple App Store
  - Google Play
  - Microsoft Store
- Not all applications are secure
  - Vulnerabilities, data leakage
- Not all applications are appropriate for business use
  - Games, instant messaging, etc.
- MDM can allow or deny app store use

Mobile Device Enforcement

Rooting/jailbreaking

- Mobile devices are purpose-built systems
  - You don't need access to the operating system
- Gaining access
  - Android - Rooting
  - Apple iOS - Jailbreaking
- Install custom firmware
  - Replaces the existing operating system
- Uncontrolled access
  - Circumvent security features, sideload apps without using an app store
  - The MDM becomes relatively useless

Mobile Device Enforcement

Carrier unlocking

- Most phones are locked to a carrier
  - You can't use an AT&T phone on Verizon
  - Your contract with a carrier subsidizes the cost of the phone
- You can unlock the phone
  - If your carrier allows it
  - A carrier lock may be illegal in your country
- Security revolves around connectivity
  - Moving to another carrier can circumvent the MDM
  - Preventing a SIM unlock may not be possible on a personal device

Mobile Device Enforcement

Firmware OTA updates

- The operating system of a mobile device is constantly changing
  - Similar to a desktop computer
- Updates are provided over the air (OTA)
  - No cable required
- Security patches or entire operating system updates
  - Significant changes without connecting the device
- This may not be a good thing
  - The MDM can manage what OTA updates are allowed

Mobile Device Enforcement

Camera use

- Cameras are controversial
  - They're not always a good thing
  - Corporate espionage, inappropriate use
- Almost impossible to control on the device
  - No good way to ensure the camera won't be used
- Camera use can be controlled by the MDM
  - Always disabled
  - Enabled except for certain locations (geo-fencing)

Mobile Device Enforcement

SMS/MMS

- Short Message Service / Multimedia Messaging Service
  - Text messages, video, audio
- Control of data can be a concern
  - Outbound data leaks, financial disclosures
  - Inbound notifications, phishing attempts
- MDM can enable or disable SMS/MMS
  - Or only allow during certain timeframes or locations

Mobile Device Enforcement

External media

- Store data onto external or removable drives
  - SD flash memory or USB/lightning drives
- Transfer data from flash
  - Connect to a computer to retrieve
- This is very easy to do
  - Limit data written to removable drives
  - Or prevent the use of them from the MDM

Mobile Device Enforcement

USB OTG

- USB On-The-Go
  - Connect mobile devices directly together
  - No computer required, only a cable
- The mobile device can be both a host and a device
  - Read from an external device, then act as a storage device itself
  - No need for a third-party storage device
- A USB 2.0 standard
  - Commonly seen on Android devices
- Extremely convenient
  - From a security perspective, it's too convenient

Mobile Device Enforcement

Recording microphone

- Audio recordings
  - There are microphones on every mobile device
- Useful for meetings and note taking
  - A standard for college classes
- A legal liability
  - Every state has different laws
  - Every situation is different
- Disable or geo-fence
  - Manage from the MDM

Mobile Device Enforcement

Geotagging/GPS tagging

- Your phone knows where you are
  - Location Services, GPS
- Adds your location to document metadata
  - Longitude, latitude
  - Photos, videos, etc.
- Every document may contain geotagged information
  - You can track a user quite easily
- This may cause security concerns
  - Take picture, upload to social media

Mobile Device Enforcement

WiFi Direct/ad hoc

- We're so used to access points
  - SSID configurations
- The wireless standard includes an ad hoc mode
  - Connect wireless devices directly
  - Without an access point
- WiFi Direct simplifies the process
  - Easily connect many devices together
  - Common to see in home devices
- Simplicity can aid vulnerabilities
  - Invisible access to important devices

Mobile Device Enforcement

Hotspot/tethering

- Turn your phone into a WiFi hotspot
  - Your own personal wireless router
  - Extend the cellular data network to all of your devices
- Dependent on phone type and provider
  - May require additional charges and data costs
- May provide inadvertent access to an internal network
  - Ensure proper security / passcode

Mobile Device Enforcement

Payment methods

- Send small amounts of data wirelessly over a limited area
  - Built into your phone
  - Payment systems, transportation, in-person information exchange
- A few different standards
  - Apple Pay, Android Pay, Samsung Pay
- Bypassing primary authentication would allow payment
  - Use proper security
  - Or disable completely

Mobile Device Deployment Models

Mobile Device Deployment Models

BYOD

- Bring Your Own Device / Bring Your Own Technology
- Employee owns the device
  - Need to meet the company's requirements
- Difficult to secure
  - It's both a home device and a work device
  - How is data protected?
  - What happens to the data when a device is sold or traded in?

Mobile Device Deployment Models

COPE

- Corporate owned, personally enabled
  - Company buys the device
  - Used as both a corporate device and a personal device
- Organization keeps full control of the device
  - Similar to company-owned laptops and desktops
- Information is protected using corporate policies
  - Information can be deleted at any time
- CYOD - Choose Your Own Device
  - Similar to COPE, but with the user's choice of device

Mobile Device Deployment Models

Corporate-owned (COBO)

- The company owns the device
  - And controls the content on the device
- The device is not for personal use
  - You'll need to buy your own device for home
- Very specific security requirements
  - Not able to mix business with home use

Mobile Device Deployment Models

VDI/VMI

- Virtual Desktop Infrastructure / Virtual Mobile Infrastructure
  - The apps are separated from the mobile device
  - The data is separated from the mobile device
- Data is stored securely, centralized
- Physical device loss - Risk is minimized
- Centralized app development
  - Write for a single VMI platform
- Applications are managed centrally
  - No need to update all mobile devices

Secure Protocols

Secure Protocols

Voice and video

- SRTP
  - Secure Real-Time Transport Protocol / Secure RTP
- Adds security features to RTP
  - Keep conversations private
- Encryption
  - Uses AES to encrypt the voice/video flow
- Authentication, integrity, and replay protection
  - HMAC-SHA1 - Hash-based message authentication code using SHA1

Secure Protocols

Time synchronization

- Classic NTP has no security features
  - Exploited as amplifiers in DDoS attacks
  - NTP has been around prior to 1985
- NTPsec
  - Secure network time protocol
  - Began development in June of 2015
- Cleaned up the code base
  - Fixed a number of vulnerabilities

Secure Protocols

Email

- S/MIME
  - Secure/Multipurpose Internet Mail Extensions
  - Public key encryption and digital signing of mail content
  - Requires a PKI or similar organization of keys
- Secure POP and Secure IMAP
  - Use a STARTTLS extension to encrypt POP3 with SSL or use IMAP with SSL
- SSL/TLS
  - If the mail is browser based, always encrypt with SSL

Secure Protocols

Web

- SSL/TLS
  - Secure Sockets Layer
  - Transport Layer Security
- HTTPS
  - HTTP over TLS / HTTP over SSL / HTTP Secure
- Uses public key encryption
  - Private key on the server
  - Symmetric session key is transferred using asymmetric encryption
  - Security and speed

Secure Protocols

File transfer

- FTPS
  - FTP over SSL (FTP-SSL)
  - File Transfer Protocol Secure
  - This is not SFTP
- SFTP
  - SSH File Transfer Protocol
  - Provides file system functionality
  - Resuming interrupted transfers, directory listings, remote file removal

Secure Protocols

LDAP (Lightweight Directory Access Protocol)

- Protocol for reading and writing directories over an IP network
  - An organized set of records, like a phone directory
- X.500 specification was written by the International Telecommunications
- Union (ITU)
  - They know directories!
- DAP ran on the OSI protocol stack
  - LDAP is lightweight, and uses TCP/IP
- LDAP is the protocol used to query and update an X.500 directory
  - Used in Windows Active Directory, Apple OpenDirectory, OpenLDAP, etc.

Secure Protocols

Directory services

- LDAPS (LDAP Secure)
  - A non-standard implementation of LDAP over SSL
- SASL (Simple Authentication and Security Layer)
  - Provides authentication using many different methods, i.e., Kerberos or client certificate

Remote access

- SSH (Secure Shell)
  - Encrypted terminal communication
  - Replaces Telnet

Secure Protocols

Domain name resolution

- DNS had no security in the original design
  - Relatively easy to poison a DNS
- DNSSEC
  - Domain Name System Security Extensions
- Validate DNS responses
  - Origin authentication, data integrity
- Public key cryptography
  - DNS records are signed with a trusted third party
  - Signed DNS records are published in DNS

Secure Protocols

Routing and switching

- SSH - Secure Shell - Encrypted terminal communication
- SNMPv3 - Simple Network Management Protocol version 3
  - Confidentiality - Encrypted data
  - Integrity - No tampering of data
  - Authentication - Verifies the source
- HTTPS
  - Browser-based management
  - Encrypted communication

Secure Protocols

Network address allocation

- Securing DHCP
  - DHCP does not include any built-in security
  - There is no “secure” version of the DHCP protocol
- Rogue DHCP servers
  - In Active Directory, DHCP servers must be authorized
  - Some switches can be configured with “trusted” interfaces
  - DHCP distribution is only allowed from trusted interfaces
  - Cisco calls this DHCP Snooping
- DHCP client DoS - Starvation attack
  - Use spoofed MAC addresses to exhaust the DHCP pool
- Switches can be configured to limit the number of MAC addresses per interface
  - Disable an interface when multiple MAC addresses are seen

Secure Protocols

Subscription services

- Automated subscriptions
  - Anti-virus / Anti-malware signature updates
  - IPS updates
  - Malicious IP address databases / Firewall updates
- Constant updates
  - Each subscription uses a different update method
- Check for encryption and integrity checks
  - May require an additional public key configuration
  - Set up a trust relationship - Certificates, IP addresses

CSF 434/534: Advanced Network and System Security

Week 06 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

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