Professor Messer's

CompTIA Security+

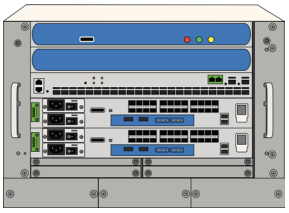
SY0-401 Study Guide

http://www.ProfessorMesser.com

Network Devices

Switch

- An OSI layer 2 device
- Hardware bridging ASICs (very fast!)
- Forwards traffic based on MAC address
- The core of an enterprise network
- High bandwidth - Many simultaneous packets

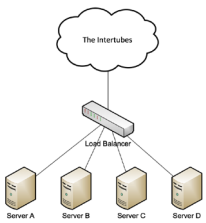


Router

- An OSI layer 3 device
- Routes traffic between IP subnets
- Routers inside of switches are sometimes called "layer 3 switches"
- Layer 2 = Switch, Layer 3 = Router
- Often connects diverse network types - LAN, WAN, copper, fiber

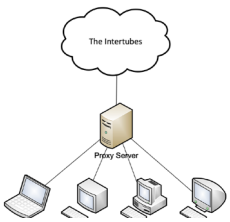
Firewall

- OSI layer 4 (TCP/UDP), some firewalls filter through OSI layer 7
- Filters traffic by port number
- Can encrypt traffic into/out of the network and between sites
- Can proxy traffic - A common security technique
- Most firewalls can be layer 3 devices (routers)



Load balancer

- Distributes the load over many physical servers
- Very common in large environments



Proxy

- Sits between the users and the external network
- Receives the user requests and sends the request on their behalf (the proxy)
- Applications may need to know how to use the proxy (explicit)
- Some proxies are invisible (transparent)

All-in-one security appliance

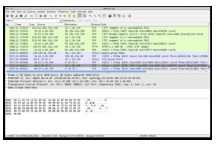
- Unified Threat Management (UTM) / Web security gateway
- URL filter / Content inspection, malware inspection, spam filter, CSU/DSU, router, switch, firewall, IDS/IPS, bandwidth shaper, VPN endpoint

VPN concentrator

- The connection point for remote users
- Traffic is encrypted across the Internet and decrypted on the internal private network

Intrusion detection/prevention system

- Protects against OS and application exploits
- Detection
  - Alerts but does not stop the attack
- Prevention
  - Blocks the attack



Protocol analyzer

- Captures network packets
- Decodes each part of the communication
- Sees all of the network conversation

Spam Filters

- Stop unsolicited email at the gateway
- Whitelist
  - Only receive email from trusted senders
- SMTP standards checking
  - Block anything that doesn't follow RFC standards
- rDNS - Reverse DNS
  - Block email where the sender's domain doesn't match the IP address
- Tarpitting
  - Intentionally slow down the server conversation
- Recipient filtering
  - Block all email not addressed to a valid recipient email address

Web Application Firewall

- Applies rules to HTTP conversations
- Allow or deny based on expected input
- Protects against exploits like SQL injections and buffer overflows
- Focus of Payment Card Industry Data Security Standard (PCI DSS)

Application-aware Security Devices

- Network-based Firewalls
  - Control traffic flows based on the application
  - Microsoft SQL Server, Twitter, YouTube
- Intrusion Prevention Systems
  - Identify the application
  - Apply application-specific vulnerability signatures to the traffic
- Host-based firewalls
  - Work with the OS to determine the application

Version 0x04

Configuring firewall rules
- Allow or disallow traffic based on security tuples
  - Source IP, Destination IP, port number, time of day, application, etc.
- Evaluated top-to-bottom
- There's an implicit deny at the bottom

VLANs
- Logically separate your switch ports into subnets
- VLANs cannot communicate to each other without a router
- Group users together by function

Secure router configuration
- Always change the default login / password
- Protect configuration file transfers
  - TFTP - in the clear
  - SCP - encrypted
  - HTTPS - encrypted

Access Control Lists (ACLs)
- Permissions associated with an object
- Used in file systems, network devices, operating systems, and more

Switch port security
- IEEE 802.1X
  - Port-based Network Access Control (PNAC)
    - Makes extensive use of EAP and RADIUS
      - Extensible Authentication Protocol
      - Remote Authentication Dial In User Service
- Disable your unused ports
- Enable duplicate MAC address checking / spoofing

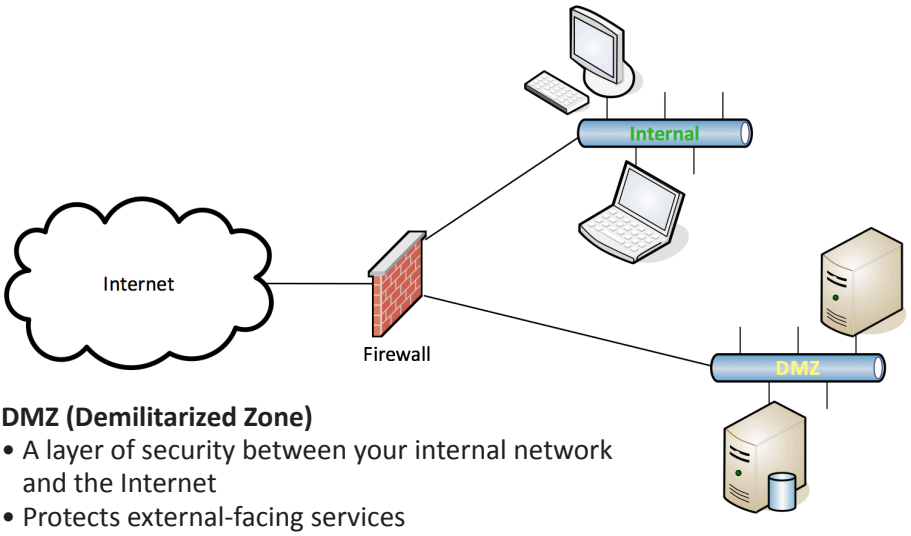
Flood Guards
- Commonly seen on intrusion prevention systems
- DoS / DDoS
  - Denial of Service
- SYN floods
  - Overload a server
- Ping floods / ping scans
  - Overwhelm the network
  - Identify what's out there
- Port floods / port scans
  - Identify open ports on a device

Spanning Tree Protocol (STP)
- IEEE standard 802.1D
- Prevents loops in bridged (switched) networks
- Built into the switch configuration options

Network Separation
- Separate switches, separate routers, no overlap
- Used in sensitive environments
- Logical separation
- Virtualization of the network infrastructure

Log Analysis
- Good for post-event analysis
- Can provide useful real-time analysis
- Automation and consolidation is the key

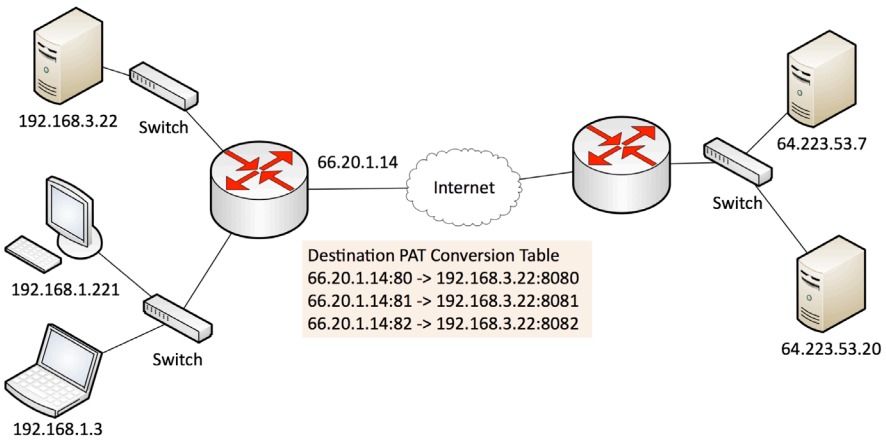
DMZ



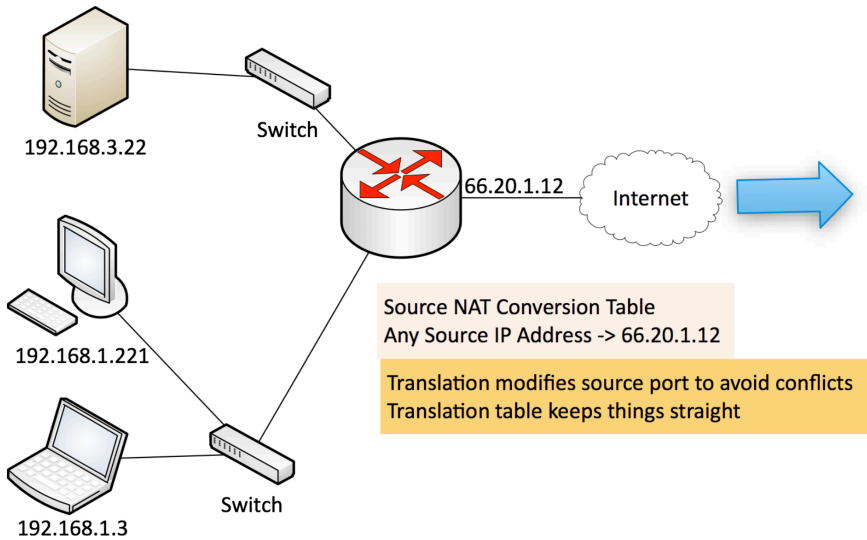
DMZ (Demilitarized Zone)
- A layer of security between your internal network and the Internet
- Protects external-facing services
- Usually less trusted than the Internal network connection

VLANs
- Logically separate your switch ports into subnets
  - VLANs cannot communicate to each other without a router
- The router/firewall becomes the gatekeeper
  - Control your organization's traffic from within
- Group users together by function
  - Be careful not to separate users too far from their resources
- Is often integrated with the NAC
  - Move people automatically into their VLAN based on credentials

Static NAT / Destination NAT



PAT (Port Address Translation) / Source NAT



Network Design

Remote Access
- An important requirement
  - We are increasingly mobile
- Take advantage of encryption technologies
  - Keep everything private
- Consider adding additional authentication technologies (One-time passwords)
- Constantly audit your access logs

Telephony
- One of the newest digital technologies
  - And one of the most difficult to secure
- Firewalls generally don't like VoIP technologies
  - You'll need protocol-specific application gateways
- Don't forget your legacy telephony!
  - Long distance still costs money

Network Access Control
- A complex technology
  - But powerful when well engineered
- Very useful in large open environments
  - Universities and large enterprises
- Requires a large security infrastructure
  - Authentication is critical
  - Redundancy is required

Virtualization
- Huge cost savings
  - Security has to catch up to the speed of change
- The control of physical objects is gone
  - Also difficult to apply external security components
- Requires additional insight
  - Harder to view intra-server communication
- Take advantage of your logs
  - They'll tell you much more than you can see

Defense in Depth
- Good security has many layers
- Firewall, DMZ, authentication, intrusion detection, VPN access, anti-virus and anti-malware software

Cloud Computing

Platform as a Service (PaaS)
- No servers, no software, no maintenance team
  - No hardware of any kind
  - Someone else handles the platform, you handle the product
- You don't have direct control of the data, people, or infrastructure
- SalesForce.com is an example of PaaS

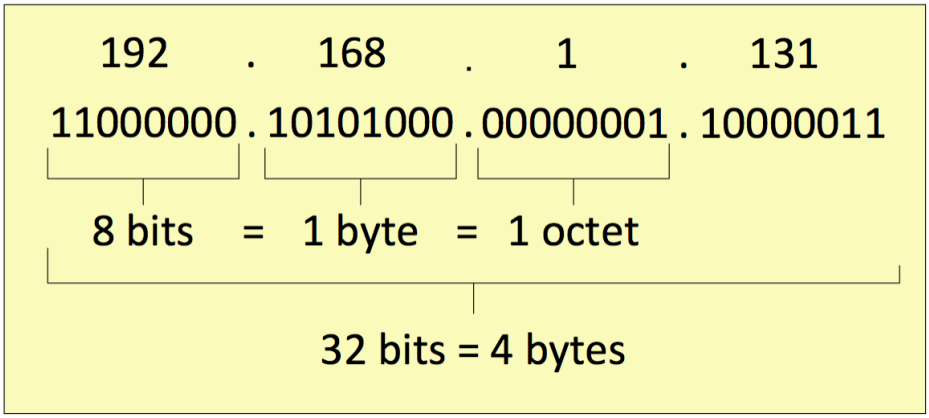
Software as a service (SaaS)
- On-demand software, no local installation
- Used for common business functions such as payroll services
- Data and applications are centrally managed
- Gmail and Google Docs is an example of SaaS

Infrastructure as a service (IaaS)
- Sometimes called Hardware as a Service (HaaS)
- Equipment is outsourced
- You are still responsible for the overall device and application management
- You're also responsible for the security
- Your data is out there, but more within your control
- Web hosting and email services would be an example of IaaS

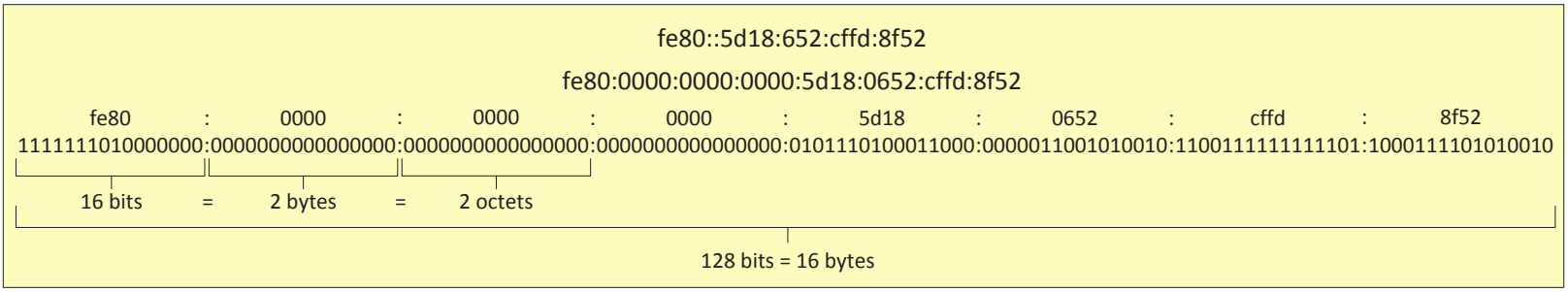
Cloud Deployment Models
- Private - A virtualized data center
- Public - Available to everyone over the Internet
- Hybrid - A mix of public and private
- Community - Several organizations share the same resources

IPv4 and IPv6

IPv4 Addressing



IPv6 Addressing



Storage Area Networking

- **Network Attached Storage (NAS)**
  - Connect to a shared storage device across the network
  - File-level access
- **Storage Area Network (SAN)**
  - Looks and feels like a local storage device
  - Block-level access

- **Fibre Channel over Ethernet (FCoE)**
  - Run Fiber Channel on Ethernet, not routable
- **Fibre Channel over IP (FCIP)**
  - Encapsulate Fibre Channel frames into IP
- **iSCSI - Internet Small Computer Systems Interface**
  - Send SCSI commands over an IP network

Ports and Protocols

Protocol	Port	Name	Description
FTP	tcp/20, tcp/21	File Transfer Protocol	Sends and receives files between systems
SSH	tcp/22	Secure Shell	Encrypted console login
SCP	tcp/22	Secure Copy	Relatively simple file copy over SSH
SFTP	tcp/22	Secure File Transfer Protocol	SSH file transfer with file management
Telnet	tcp/23	Telecommunication Network	Remote console login to network devices
DNS	udp/53, tcp/53	Domain Name Services	Convert domain names to IP addresses
TFTP	udp/69	Trivial File Transfer Protocol	A very simple file transfer application
HTTP	tcp/80	Hypertext Transfer Protocol	Web server communication
NetBIOS	udp/137, udp/138	Network Basic Input/Output System	NetBIOS over UDP - Name service, Datagram service
NetBIOS	tcp/139	Network Basic Input/Output System	NetBIOS over TCP - Session service
IMAP	tcp/143	Internet Message Access Protocol	Retrieve and store email
SNMP	udp/161	Simple Network Management Protocol	Gather statistics and manage network devices
TLS/SSL	tcp/443	Transport Layer Security and Secure Sockets Layer	Secure protocols for web browsing
HTTPS	tcp/443	Hypertext Transfer Protocol Secure	Web server communication with encryption
FTPS	tcp/990, tcp/989	FTP over SSL	Adds security to FTP with TLS/SSL
ICMP	N/A	Internet Control Message Protocol	Management protocol
IPsec	Various	Internet Protocol Security	Authentication, integrity, confidentiality, and encryption

OSI Model

OSI Mnemonics

- Please Do Not Trust Sales Person's Answers
- All People Seem To Need Data Processing
- Please Do Not Throw Sausage Pizza Away!

Layer 7 - Application	The layer we see - Google Mail, Twitter, Facebook
Layer 6 - Presentation	Encoding and encryption (SSL / TLS)
Layer 5 - Session	Communication between devices (control protocols, tunneling protocols)
Layer 4 - Transport	The "post office" layer (TCP segments, UDP datagrams)
Layer 3 - Network	The routing layer (IP addresses, routers, packets)
Layer 2 - Data Link	The switching layer (frames, MAC addresses, EUI-48, EUI-64, switches)
Layer 1 - Physical	Signaling, cabling, connectors (cables, NICs, hubs)

Wireless Encryption and Authentication

EAP (Extensible Authentication Protocol)
- An authentication framework
- WPA and WPA2 use five EAP types as authentication mechanisms

LEAP (Lightweight Extensible Authentication Protocol)
- Cisco proprietary
- Uses passwords only
- No detailed certificate management
- Based on MS-CHAP (including MS-CHAP security shortcomings)

PEAP (Protected Extensible Authentication Protocol)
- Created by Cisco, Microsoft, and RSA Security
- Encapsulates EAP in a TLS tunnel
- Only one certificate needed, on the server

WEP
- 64-bit or 128-bit key size
- Cryptographic vulnerabilties found in 2001
- WEP is no longer used

WPA
- Short-term workaround after WEP
- Used RC4 cipher as a TKIP (Temporal Key Integrity Protocol)
- TKIP has its own vulnerabilities

WPA2
- Replaced TKIP with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
- Replaced RC4 with AES (Advanced Encryption Standard)
- WPA2 is the latest and most secure wireless encryption method

WPA2-Enterprise
- WPA2-Enterprise adds 802.1x
- RADIUS server authentication

Wireless Security

Captive Portal
- Authentication to a network
  - Common on wireless networks
- Access table recognizes a lack of authentication
  - Redirects your web access to a captive portal page
- Username / password
  - And additional authentication factors
- Once proper authentication is provided, the web session continues
  - Until the captive portal removes your access

Omnidirectional Antennas
- One of the most common
  - Included on most access points
- Signal is evenly distributed on all sides
  - Omni=all
- Good choice for most environments
  - You need coverage in all directions
- No ability to focus the signal
  - A different antenna will be required

Directional Antennas
- Focus the signal - Increased distances
- Send and receive in a single direction
  - Focused transmission and listening
- Antenna performance is measured in dB
  - Double power every 3dB of gain
- Yagi antenna - Very directional and high gain
- Parabolic antenna - Focus the signal to a single point

MAC (Media Access Control) filtering
- Access is controlled through the physical hardware address
- It's easy to find a working MAC addresses through wireless LAN analysis
- MAC addresses can be spoofed
- Security through obscurity

SSID (Service Set Identifier) Management
- The SSID is the name of the wireless network
  - i.e., LINKSYS, DEFAULT, NETGEAR
- Change the SSID to something appropriate for its use
- The SSID broadcasts can be disabled
- You can still determine the SSID through wireless network analysis
- Security through obscurity

Temporal Key Integrity Protocol
- Created when WEP was broken
  - We needed a stopgap to make 802.11 stronger
- Mixed the keys - Combines the secret root key with the IV
- Adds sequence counter - Prevents replay attacks
- 64-bit Message Integrity Check - Protects against tampering
- Used in WPA (Wi-Fi Protected Access) prior to the creation of WPA2

CCMP
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
  - Replaced TKIP when WPA2 was published
- A more advanced security protocol
  - Based on AES and uses a 128-bit key and a 128-bit block size
  - Requires additional computing resources
- Data confidentiality - Only authorized parties can access the information
- Authentication - Provides proof of genuineness of the user
- Access control - Allow or disallow access to the network

Site Surveys
- Sample the existing wireless spectrum
- Identify existing access points
- Work around existing frequencies - layout and plan for interference
- Plan for ongoing site surveys - things will certainly change

VPN over Wireless Networks
- Wireless from your local coffee shop - no encryption
- Everyone around the coffee shop can see your traffic
- Exceptionally easy to capture your data
- Some of your data might be encrypted with HTTPS. Maybe.
- Protect all of your traffic with a VPN tunnel

Dealing with Risk

Control types
- Technical security controls
  - Access control, audit and accountability, identification and authentication, system and communications protection
- Management security controls
  - Security assessment and authorization, planning, risk assessment, system and services acquisition, program management
- Operational security controls
  - Awareness and training, configuration management, contingency planning, incident response, maintenance, media protection, physical and environmental protection, personnel security, system and information integrity

False Postitives
- A report that isn't true - a false alarm or mistaken identity
- IDS/IPS information - only as good as the signatures
- Workstation anti-virus - False positives can remove legit files
- Consider a second opinion - http://www.VirusTotal.com

False Negatives
- A report missed identifying something - no notification
- Malicious traffic got through your defenses
- It's difficult to know when this happens - It's completely silent
- Get catch/miss rates with industry tests - IPS, anti-virus

Security policies
- A set of policies that covers many areas of security
  - Human resource policies
  - Business policies
  - Certificate policies
  - Incident-response policies

Risk Calculation
- Annualized Rate of Occurrence (ARO)
  - How likely is it that a hurricane will hit? In Montana? In Florida?
- SLE (Single Loss Expectancy)
  - What is the monetary loss if a single event occurs?
  - Laptop stolen = $1,000
- ALE (Annual Loss Expectancy)
  - ARO x SLE
  - 7 laptops stolen a year (ARO) x $1,000 (SLE) = $7,000
- The business impact can be more than monetary
  - Quantitative vs. qualitative

Quantitative Risk Assessment
- Assign a dollar value to risk
- Single Loss Expectancy (SLE) - How much loss for one event?
- Annual Loss Expectancy
  - SLE x Annual Rate of Occurrence (ARO)
- Often difficult to calculate without historical reference
  - How risky is a buffalo stampede?

Qualitative Risk Assessment
- Identify significant risk factors
- Ask opinions about the significance
- Display visually with traffic light grid or similar method

Threat Assessment
- Where are we vulnerable to threats?
  - OS, applications, 3rd-party connections, Internet
- Constant vigilance
  - New threats discovered all the time
  - Old threats become popular again

Vulnerability Assessment
- Actively scan a network in search of vulnerabilities
  - Known vulnerabilities
  - Automated process
  - For unknown vulnerabilities, consider input validation/fuzzing
- Can identify obvious and no-so-obvious vulnerabilities
  - Lack of application/OS patches
  - No anti-virus/anti-spyware
  - Weak passwords

Vulnerabilities
- A flaw or weakness
  - A door with a broken lock
  - An operating system library that grants administrative access
- This doesn't mean your system has been breached
  - Someone first has to know about the vulnerability
  - Some vulnerabilities were there, but previously unknown
- This is why we patch
  - New vulnerabilities are identified all the time

Threat Vectors
- The path that the threat takes to the target
  - Target: Your computer, mobile device, gaming system
- Email: Embedded links, attached files
- Web browser: Fake site, session hijack
- Wireless hotspot: Rogue access point
- Telephone: Social engineering
- USB flash drive: Auto-executing malware
- And many more…

Threat Probability
- Identify actual and potential threats
  - Regardless of the probability
- Identify as many vulnerabilities as possible
  - Check your OS, your services, and your applications
  - Nobody said this would be easy
- Now you can calculate the likelihood of a successful exploit
  - There's no official formula here
  - Different organizations will have different priorities

Deflecting Risk
- Risk-avoidance
  - Stop participating in high-risk activity
- Risk transference
  - Buy some insurance
- Risk acceptance
  - A business decision; we'll take the risk!
- Risk mitigation
  - Decrease the risk level
- Risk deterrence
  - Big dogs, security fences, warning signs

Dealing with Risk (continued)

Risks with Cloud Computing
- Control of data
  - Data in the cloud can potentially be accessed by anyone
- Security is managed elsewhere
  - Your control mechanisms are in the hands of others
- Server unavailability / Account lockout
  - Cloud computing doesn't guarantee availability

Risks associated with virtualization
- Compromising the virtualization layer puts all systems at risk
- There is little control over VM to VM communication
  - Support for "virtual firewalls" is an emerging technology
- Single physical host contains VMs that have different security profiles
- Physical separation is no longer possible
- There is potential for loss of separation of duties
  - System admin controls many servers on a single piece of hardware

Recovery Time Objectives
- Mean time to restore (MTTR)
  - Mean time to repair
- Mean time to failure (MTTF)
  - The expected lifetime of a product or system
- Mean time between failures (MTBF)
  - Predict the time between failures
- Recovery time objectives (RTO)
  - Get up and running quickly
  - Get back to a particular service level
- Recovery point objectives (RPO)
  - How much data loss is acceptable?
  - Bring the system back online; how far back does data go?

Integrating Systems and Data with Third Parties

On-boarding
- Bring a new partner into the organization
  - This is more particular than hiring new staff
- Many agreements will be in place
  - Legalities associated with business and security matters
- Implement technical functions
  - Secure connections between partners
- Usually as an IPsec tunnel or physical segmentation
  - Establish an authentication method
    - Provide access to shared resources
  - Audit all security controls
    - Properly share (and separate) data

Off-boarding
- This process should be pre-planned
  - You don't want to decide how to do things at this point
- How will the systems be dissolved?
- What happens to the data?
- When will the final connections be terminated?

Social Media and Third-Party Concerns
- Management of data
  - Social media data includes privacy concerns
  - Some of the data is extremely valuable
- Your social media reputation
  - Someone else is tweeting for you
  - The tone is as important as the message
- Account control is important
  - Social media accounts are shared by a large group
  - A mistake on one phone can be seen by many

Interoperability Agreements
- Memorandum of Understanding
  - Informal letter of intent;not a signed contract
  - Usually includes statements of confidentiality
- Service Level Agreement (SLA)
  - Minimum terms for services provided
  - Uptime, response time agreement, etc.
- Business Partners Agreement (BPA)
  - Commonly seen between manufacturers and resellers
- Interconnection Security Agreement (ISA)
  - Used by US Federal Government to define security controls

Privacy Considerations
- Privacy of the individual
  - Both personal and professional
- Legally mandated privacy laws in many European countries
  - An employer can't track your personal computer use
- Customer data often contains a aspect of privacy
  - Even benign data can be combined to violate privacy
- Third-party agreements must consider privacy
  - The rules should be in place from the beginning

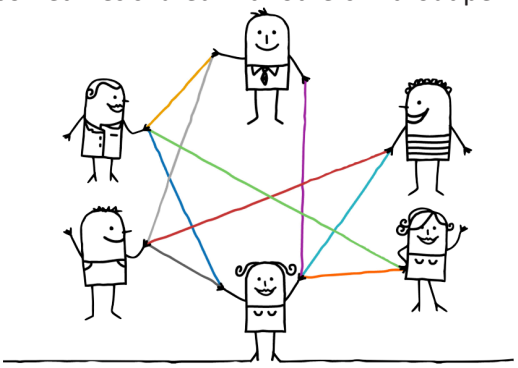
Data Ownership
- Data is everything
  - The most important asset in an organization
  - Without the data, there's no company
- The owner of the data has a responsibility
  - Protection, privacy
  - Technical / Logical controls
  - Physical controls
- Who owns the data if the third-party agreement ends?
  - This should be determined prior to that circumstance

Risk Awareness with Third-Parties
- Combine two systems
  - Hopefully get a seamless technical integration
- Security must be designed into the project
  - Usually designed by teams from both organizations
  - Everyone must be aware of the risks
- Security policies must be examined for additional risks
  - Resources, business requirements, and risk must be balanced
- Agreements must be in place
  - For example: Who does backups?
    Who gets access to the backups? How are the backups stored?

Data Ownership
- Who owns the data?
  - There's more than one participant
  - Is there more than one owner?
  - What part of the data is owned by which partner?
- Data ownership agreements can avoid some of the messy details
  - Where is the data stored?
  - Who owns the data when
  - the relationship is over?
  - How is data destroyed?

Integrating Systems and Data with Third-Parties (continued)

Third-party Data Sharing
- Data shared between partners
  - Network connections may exist
  - Proper controls may not be in place
- Data shared with others
  - Agreements are usually in place with the data owners
  - Data is sometimes shared with others without permission



Data Backups with Third-Parties
- Backups are often overlooked
  - They contain everything
- Data backups are often kept off-site
  - Yet-another third-party
- Losing data from a backup is a very bad thing
  - Seems to happen more often than you might think
- Not all backups are the same
  - Financial data, health care data, top secret data, etc.

Security Policy Considerations with Third-parties
- The security policy is the weakest link
  - A badly implemented security policy puts data at risk
- Protect information between vendors, partners, and customers
  - Avoid data modification, disclosure, damage, or destruction
- Most of this language is contractual
  - Everybody understands their responsibilities
- Security policies are constantly updated
  - The threat landscape is constantly changing

Third-Party Security Compliance
- Third-party relationships add to the need for security compliance
  - Shared resources require additional oversight
- Compliance can be technically challenging
  - Cloud-based services add additional complexity
- Some compliance requirements are legally mandated
  - HIPAA - Health Insurance Portability and Accountability Act
  - PCI DSS - Payment Card Industry Data Security Standard
  - FISMA - Federal Information Security Management Act
- Perform a gap analysis
  - Determine all gaps in security
- Resolve the issues
  - Some issues can't be easily resolved
  - A decision must be made regarding cost vs. benefit
- Perform periodic audits
  - These audits may be involved and far-reaching
  - More coordination required with the third-party

Mitigating Risk

Change Management
- Upgrade software, change firewall configuration, modify switch ports
- Occurs very frequently
- The change management process is often overlooked or ignored
- Clear policies are needed
- Frequency, duration, installation process, fallback procedures

Incident Management
- Series of events that negatively affects the organization
  - Database hack, stolen laptop, water pipe burst
- Who will be contacted when an incident occurs?
- Who's responsible for managing the incident response?
- Technical steps for handling systems and preserving evidence
- What goes on the report?

User Rights and Permissions
- Management sets the limits
- Security team administers the limits
- You must translate management requirements into technical access
- Periodic audits are useful

Auditing
- Does everyone have the correct permissions?
- How are your resources used?
- Are your systems and applications secure?
- Are your disaster recovery plans going to work?
- Can you contact the right people at the right time?
- Document everything

Preventing data loss or theft
- Involves process and procedure
- Some of the most difficult data policies to implement
  - It's very easy to carry large amounts of data around
- There are both internal and external threats
- You have to protect everywhere
- This is a bigger threat every day

Data Loss Prevention Systems
- On your computer - Data in use
- On your network - Data in motion
- On your server - Data at rest

Basic Forensic Procedures

Most Volatile	CPU registers, CPU cache
	Router table, ARP cache, process table, kernel statistics, memory
	Temporary file systems
	Disk
	Remote logging and monitoring data
	Physical configuration, network topology
Least Volatile	Archival media

Capturing system images
- Copy the contents of a disk
  - Bit-for-bit, byte-for-byte
- Software imaging tools
  - Use a bootable device
- Remove the physical drive
  - Use a hardware write-blocker
- Get the backup tapes
  - These may already be available

Basic Forensic Procedures (continued)

Capturing System Images
- Copy the contents of a disk
  - Bit-for-bit, byte-for-byte
  - Get every morsel of information
- Software imaging tools
  - Use a bootable device
- Remove the physical drive
  - Use a hardware write-blocker
- Get the backup tapes
  - Some of this work may have been done for you

Network traffic and logs
- Traffic logs
- Firewalls log a lot of information
- Switches and routers don't usually log user-level information
- Intrusion Detection/Prevention Systems
- Raw network traffic data
  - Rebuild images, email messages, browser sessions, file transfers

Capture video
- A moving record of the event
- Gathers information external to the computer and network
- Captures the status of the screen and other volatile information

Time Offsets
- Windows: 64-bit time stamp
  - Number of 100-nanosecond intervals since January 1, 1601 00:00:00 GMT
  - This stops working in 58,000 years
- Unix: 32-bit time stamp
  - Number of seconds since January 1, 1970 00:00:00 GMT
  - This stops working on Tuesday, January 19, 2038 at 3:14:07 GMT
- Different file systems store timestamps differently
  - FAT: Time is stored in local time
  - NTFS: Time is stored in GMT
- Record the time offset from the operating system
  - The Windows Registry
  - Many different values (daylight saving time, time change information, etc.)

Taking Hashes
- MD5 (Message Digest 5)
  - 128 bits, displayed as hexadecimal
- CRC (Cyclical Redundancy Check)
  - 32 bits, displayed as hexadecimal
- Create an MD5 hash for an image, file, or groups of files
  - Data can be verified at any time
- Don't forget security cameras
- The video content must also be archived

Screenshots
- Capture the state of the screen
  - Difficult to reproduce, even with a disk image
- External capture
  - Use digital camera
- Internal capture
  - PrintScreen key
- Third-party utility

Witnesses
- Who might have seen this?
- Interview and document
- Not all witness statements are 100% accurate
- Humans are fallible

Tracking man hours and expense
- Some incidents can use massive resources
- May have an impact on the bottom line
- May be required for restitution
- Be as accurate as possible

Chain of custody
- Controlling and manging the evidence to maintain integrity
- Document everyone who contacts the evidence
- Use hashes with digital evidence
- Label and catalog everything
- Seal, sign, and store

Big Data Analysis
- Large amounts of data, stored without structure
- Incidents can create an enormous amount of data
- Diverse log formats and data types
- Collecting the data is only the first part
  - You must also be able to view it
- Query the data
  - A structured language that applies to large scale data
- Visualization tools can display the data in unique ways
  - Graphs
  - Statistical analysis
  - Tag clouds

Incident Response Procedures

Preparing for an Incident
- Communication methods - phones and contact information
- Incident handling hardware and software
  - Laptops, removable media, forensic software, digital cameras
- Incident analysis resources
  - Documentation, network diagrams,baselines, critical file hash values
- Incident mitigation software -
  - Clean OS and application images
- Policies needed for incident handling
  - Everyone knows what to do

Preventing an Incident
- Risk assessments
  - Periodic analysis, prioritization of risk, disposition of risk
- Host security
  - Harden the operating system, patches, and ongoing monitoring
- Network security
  - Firewalls, VPNs, intrusion prevention systems
- Malware prevention
  - Hosts, email and file servers, application clients
- User awareness and training
  - Keep your users updated with the latest security techniques

Incident Precursors
- Web server log
  - Vulnerability scanner in use
- Exploit announcement
  - Monthly Microsoft patch release, Adobe Flash update
- Direct threats
  - A hacking group doesn't like you

Incident Indicators
- An attack is underway or an exploit is successful
- Buffer overflow attempt
  - Identified by an intrusion detection/prevention system
- Anti-virus software identifies malware
  - Deletes from OS an notifies administrator
- Host-based monitor detects a configuration change
  - Constantly monitors system files
- Network traffic flows deviate from the norm
  - Requires constant monitoring

Incident Notification
- Corporate / Organization
  - CIO / Head of Information Security / Internal Response Teams
- Internal non-IT
  - Human resources, public affairs, legal depatment
- External contacts
  - System owner, law enforcement
  - US-CERT (for U.S. Government agencies)

Event Notification
- Notification is ongoing during an event
  - Status updates, wide-scale notifications
  - Consider in-band and out-of-band methods
- Email, Web (intranet, external, etc.), Telephone calls, In-person updates, Voice mail recordings, Paper flyers, notices

Criteria for Mitigation Strategies
- Potential damage and theft - prevent the destruction
- Preserve the evidence - gather as many details as possible
- Maintain service availability - The organization must continue
- Implementation resources and time - Every task requires resources
- Effectiveness - amount of containment
- Duration of the mitigation - Let's get this over quickly

Isolation and Containment
- Generally a bad idea to let things run their course
  - An incident can spread quickly
- Sandboxes
  - The attacker thinks they're on a real system, but they're not
- Isolation can be sometimes be problematic
  - Malware or infections can monitor connectivity
  - When connectivity is lost, everything is deleted/encrypted/damaged

Lessons Learned from Incidents
- What happened, exactly?
  - Timestamp of the events
- How did your incident plans work?
  - Did the process operate successfully?
- What would you do differently next time?
  - Retrospective views provide context
- Which indicators would you watch next time?
  - Different precursors may give you better alerts

Incident Reporting
- A lot of information is created during an incident
  - Information should be objective and factual
- Logbook - a pencil and paper is remarkable technology
- Digital camera - a snapshot or movie of a device
- Audio recorder - easier to say it and transcribe later
- Laptop - capture terminal sessions and digital evidence

Tracking Issues
- Incident status
- Summary information
- Relationship between incidents
- Actions taken by all parties
- Chain of custody information
- Contact information
- Comments from incident handlers
- Next steps to be taken

Incident Recovery
- Eradicate the bug
  - Remove malware, disable breached user accounts, fix vulnerabilities
- Recover the system
  - Restore from backups, rebuild from scratch, replace compromised files, tighten down the perimeter

Reconstitution
- A phased approach - it's difficult to fix everything at once
- Recovery may take months
  - Large-scale incidents require a large amount work
- The plan should be efficient
  - Start with quick, high-value security changes
    - Patches, firewall policy changes
  - Later phases involve much "heavier lifting"
    - Infrastructure changes, large-scale security rollouts

First Responders
- Very specific tasks for the first person on the scene
- Objective is to contain the damage
- Don't disturb the environment
- Get the right people in place before poking around
- Follow the escalation policy

Handling a Data Breach
- Try to determine the attacker
  - Useful for law enforcement and to stop future breaches
- Security must be analyzed and secured
  - Change passwords, update firewalls
  - Even across systems that may not appear to be breached
- Notify all affected people - customers, partners, employees
- Personally Identifiable Information (PII) may require additional notifications
  - Credit monitoring requirements

Damage and Loss Control
- Prevent the spread of damage
  - Needs to be part of the incident response policy
- Virus infection may be handled differently than a DoS attack
  - Device removal - pull a device from the network
  - Disconnect the Internet
- Every case is a bit different
  - What's attacked or damaged?
  - Can you gather additional details if you leave it in place?

Security-Related Awareness and Training

Security policy training and procedures
- All of your policy information is on the Intranet
- Provide in-person mandatory training sessions
- Train people on general security best practices
- Define a company policy for visitors GUI configuration

Personally identifiable information (PII)
- Part of your privacy policy
- Not everyone realizes the importance of this data
- It should become a normal part of security management

Information classification examples
- Unclassified (public) - no restrictions on viewing the data
- Classified (private / restricted / internal use only) - restricted
- Confidential (low) - highly sensitive, must be approved to view
- Secret (medium) - viewing is severely restricted
- Top-Secret (high) - highest level of classification

Data labeling, handling and disposal
- Data is usually saved for a very long time
- Document and label everything
- Some backups must be legally preserved
- Trash and recycling can be a security concern

Compliance, best practices and standards
- Non-compliance has serious repercussions
- Sarbanes-Oxley Act (SOX) - The Public Company Accounting Reform and Investor Protection Act of 2002
- The Health Insurance Portability and Accountability Act (HIPAA)
  - Extensive 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

User habits
- Promote good password behaviors
- Document data handling processes
- Define clean desk policies
- Personally owned devices can be a challenge
- Tailgating can allow unauthorized people to enter the building

Threat Awareness
- New viruses - thousands every week
- Phishing attacks
- Spyware
  - Learns personal info, captures keystrokes & browsing information
- Zero-day exploits
  - Quick reaction is the only defense

Social networking and P2P
- You become a file server
- All of your content can be exposed
- Social networks provide false sense of trust

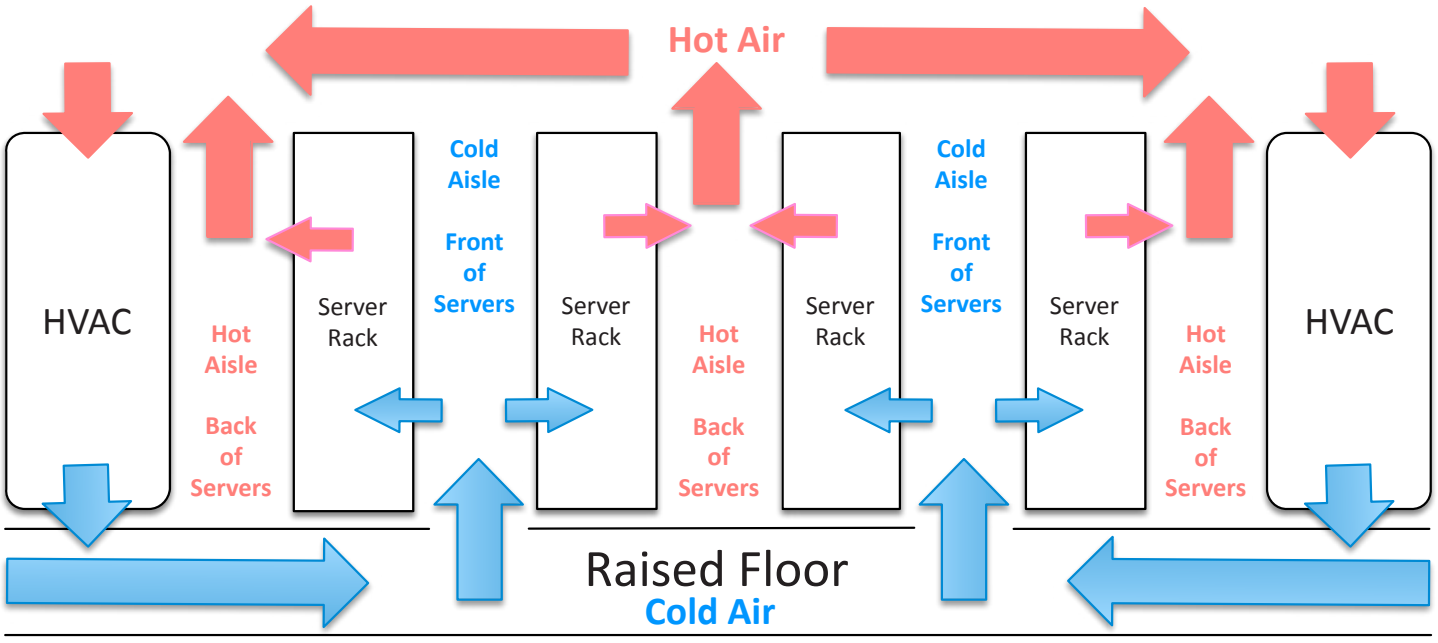
Gathering Training Metrics
- Formative assessment
- Constant monitoring, target areas that need work
- Summative assessment
- High-stakes, final exam, certification exam

Automating Training Measurements
- Large-scale monitoring - automation is the key
- Learning Management System (LMS) assessment software
- Training delivery- video, text, quizzes
- Score tracking - individual performance
- Student feedback - communication path to the trainers

Physical Security and Environmental Controls

HVAC (Heating, Ventilating, and Air Conditioning)
- Thermodynamics, fluid mechanics, and heat transfer
- Not something you can properly design yourself
- Must be integrated into the fire system
- Data Center should be separate from the rest of the building
- Overheating is a huge issue
- Engineer for closed-loop recirculating and positive pressurization
- Recycle internal air and air is pushed out

Fire Suppression
- Electronics require unique responses to fire
  - Water is generally a bad thing
- Identify with smoke detector, flame detector, heat detector
- Suppress with water / dry pipe, wet pipe, preaction
- Suppress with chemicals
  - Halon is no longer manufactured
  - Use Dupont FM-200 / American Pacific Halotron



Physical Security and Environmental Controls (continued)

Electromagnetic Interference Shielding
- Computers produce large amounts of EMI
- Metal shielding inside of a computer case can minimize EMI
- Appears as noise on video and analog audio

Environmental Monitoring
- Optimize your cooling infrastructure
- Constantly monitor and log the environment
- Many servers include internal temperature sensors
- Portable or emergency cooling may be valuable

Physical Security
- Hardware locks - Lock and key, deadbolt, electronic, token-based, biometric, multi-factor smart card
- Mantraps - Multiple doors that only unlock one at a time
- Video surveillance - closed-circuit television
- Fencing - a perimeter
- Proper lighting - deter crime and provide camera lighting
- Signs - specific instructions, fire exits, warning signs
- Guards - access lists, physical protection
- Barricades - channel people through a particular access point
- Protected Distribution System (PDS) - physically secured cabling
- Alarms - circuit-based, motion detection

Control Types
- Technical - access control, audit and accountability, identification and authentication, system and communications protection
- Management - security assessment and authorization, planning, risk assessment, system and services acquisition, program management
- Operational - awareness and training, configuration management, contingency planning, incident response, maintenance, media protection, physical and environmental protection, personnel security, system and information integrity

Risk Management Best Practices

Business Impact Analysis
- What are your critical business functions?
- Is there loss of revenue, legal requirements, or customer service?
- How long will you be impacted?
- What's the impact to the bottom line?

Critical Systems
- Make a list of critical systems - this is an involved process
- List business processes - Accounting systems, manufacturing application, VoIP call center, etc.
- Associate tangible and intangible assets and resources with the business processes

Tangible and Intangible Assets
- People - employees, suppliers, visitors
- Tangible assets - buildings, furniture, equipment, data, paper documents
- Intangible assets - Ideas, commercial reputation, brand
- Procedures - Supply chains, critical procedures, standard operating procedures

Removing Single Points of Failure
- A single event can ruin your day
- Network redundancy with multiple devices
- Backup power, multiple cooling devices
- Plan for additional people and other locations
- There's no practical way to remove all points of failure

Quantitative Risk Assessment
- Assign a dollar value to risk
- Single Loss Expectancy (SLE) - How much loss for one event?
- Annual Loss Expectancy - SLE x Annual Rate of Occurrence (ARO)

Qualitative Risk Assessment
- Identify significant risk factors
- Ask opinions about the significance
- Display visually with traffic light grid or similar method

Continuity of operations
- Business processes are interrelated
  - HR drives payroll, IT provides payroll system, accounting provides the money
- Almost everything business-related relies on IT
- Involve the entire company
- It can be difficult to document the company operations

Disaster Recovery
- Plan for both small disasters and large disasters
- Can be managed through a 3rd-party
- Take advantage of geographically diverse areas
- Many variables, the unknown can bite you

Seven-step contingency planning process
- Develop the contingency planning policy statement
- Conduct the business impact analysis
- Identify preventive controls
- Create contingency strategies
- Develop an information system contingency plan
- Ensure plan testing, training, and exercises
- Ensure plan maintenance

Succession Planning
- Manage the leadership of the company
  - A gap can cause a vacuum or financial impact
- Management can leave the company, retire, die
- Often a deputy who can assume the role
- Travel restrictions may apply

Tabletop Exercises
- Performing a full-scale disaster drill can be costly
- Many of the logistics can be determined through analysis
  - You don't physically have to go through a disaster or drill
- Get key players together for a tabletop exercise
  - Talk through a simulated disaster

Risk Management Best Practices (continued)

Redundancy and Fault Tolerance
- Maintain uptime - the organization continues to function
- No hardware failure - servers keep running
- No software failure - services always available
- No system failure - network performing optimally

High Availability
- Redundancy doesn't always mean always available
- HA (high availability) - always on, always available
- May include many different components working together
- Watch for single points of failure

Hot, Warm, and Cold Spares
- Cold spare - in the box, turned off
- Warm spare - may be racked and powered, but not connected
  - Software and configurations may occasionally be updated
- Hot spare - powered on, always updated

Cold, Warm, and Hot Sites
- Cold site - no hardware, no data, no people
- Warm site - hardware is waiting, you bring the data
- Hot site - an exact replica, stocked with hardware and software
  - Flip a switch and everything moves

RAID Levels

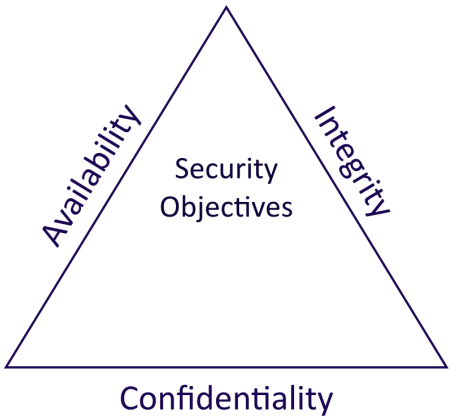
RAID Level	Description	Details
RAID 0	Striping without parity	High performance, no fault tolerance
RAID 1	Mirroring	Duplicates data for fault tolerance, but requires twice the disk space
RAID 5	Striping with parity	Fault tolerant, only requires an additional disk for redundancy
RAID 0+1, RAID 1+0, RAID 5+1, etc.	Multiple RAID types	Combine RAID methods to increase redundancy

Security Goals

Confidentiality
- Certain information should only be known to certain people
- Encryption - Encode messages so only certain people can read it
- Access controls - Selectively restrict access to a resource
- Steganography
  - Conceal information within another piece of information
  - Commonly associated with hiding information in an image

Integrity
- Data is stored and transferred as intended
  - Any modification to the data would be identified
- Hashing - Map data of an arbitrary length to data of a fixed length
- Digital signatures - Verify the integrity of data
- Certificates - Combine with a digital signature to verify an individual
- Non-repudiation - Provides proof of integrity

Availability
- Information is accessible to authorized users
- Redundancy - Build services that will always be available
- Fault tolerance - System will continue to run with failures
- Patching - Stability, close security holes



Safety
- Fencing - Keep out the unwanted
- Lighting - Protect assets, especially at night
- Locks - Prevent access through doors
- CCTV - Closed-circuit television - video camera monitoring
- Escape plans and routes - Best way out of an area
- Drills - Test and adjust
- Testing controls - Test against physical and digital security

Malware Types

Malware
- Can gather information
- Can capture your keystrokes
- Often controlled over the 'net
- Can show you advertising
- May install an OS backdoor

Virus
- Malware that can reproduce itself
- It doesn't need you to click anything
- It needs you to execute a program
- Reproduces through file systems or the network
- Just running a program can spread a virus
- Some viruses are invisible, some are annoying
- Anti-virus software is very common
- There are thousands of new viruses every week

Virus Types
- Boot sector viruses
  - Installs into the drive boot area
- Program viruses
  - Part of a legitimate application
- Script viruses
  - Operating system and browser-based
- Macro viruses
  - Common in Microsoft Office
- Multipartite viruses - Infects and spreads in multiple ways

Worms
- Malware that self-replicates without human intervention
- Uses the network as a transmission medium
- Can infect many PCs very quickly
- Firewalls and IDS/IPS can mitigate many worm infestations

Adware
- Your computer shows you advertisements
- May cause performance issues
- May be included with other software installations
- Be careful of software that claims to remove adware

Spyware
- Malware that spies on you
- Advertising, identity theft, affiliate fraud
- Can trick you into installing
- Monitors your browser activity
- Logs your keystrokes
- Send this information back to a central server

Trojan Horse
- Software that pretends to be something else
- Replicating isn't the primary reqirement
- Circumvents your existing security because you ran it yourself
- Anti-virus may catch it when it runs
- The better trojans are built to avoid and disable AV
- Once it's inside it has free reign
- May then open the gates for other programs

Backdoors
- Why go through normal authentication methods? Just walk in the back door
- Often placed on your computer through malware
- Some malware software can take advantage of backdoors created by other malware
- Bad software can have a backdoor as part of the app

Rootkits
- Modifies core system files
- May be part of the kernel
- Designed to be invisible to the operating system
  - You won't see it in Task Manager
- Also invisible to traditional anti-virus utilities

Logic Bomb
- Waits for a predefined event
- Time bomb - Based on time or date
- Logic bomb - Set off through a user event
- Difficult to identify
- Difficult to recover if it goes off

Botnets
- Robot networks
- Once your machine is infected, it becomes a bot
- You usually do not know that you're a bot
- May be installed as part of a malware
- Waits around until receiving commands from the mothership

Ransomware
- The bad guys want your money
  - They'll take your data in the meantime
- May be a "fake" ransom
  - Locks your computer "by the police"
- The ransom may be avoided
  - A security professional can remove these kinds of malware

Polymorphic Malware
- Changes itself to avoid signature detection
  - Every download is different
- The attack code doesn't change
  - Just everything around it
- Encrypt the malware executable
  - Use a different key pair every time
- Create signatures that look for a specific payload
  - One signature can stop many variants
- Use heuristic detection systems
  - Be ready to use some additional resources

Armored Virus
- Virus writers don't want their work to be discovered
  - Makes the anti-virus software look elsewhere
- If found, make it difficult to deconstruct
  - Security researchers disassemble the virus code
  - The virus is usually obfuscated with unnecessary and nonsense code
- The virus writer's goal is to make it as painful as possible to identify and block
  - The longer the research, the more widespread the infection

Attack Types

ARP Poisoning, Spoofing, and Man-in-the-Middle
- Redirects your traffic, then passes it on to the destination
- You never know your traffic was redirected
- ARP has no security, relies on security in the switch

Denial of service
- Force a service to fail
- Overload the service
- Take advantage of a design failure or vulnerability
- Cause a system to be unavailable
- Can be used to create a smokescreen for some other exploit
- May be a precursor to a DNS spoofing attack
- Not usually a very complicated attack
- Turning off your power is an uncommon but effective DoS

Replay Attack
- Useful information is transmitted over the network
- Network Tap is used to access to the raw network data
- ARP poisoning can redirect traffic
- Malware on the victim computer gathers information
- Data is replayed to appear as someone else

Spoofing
- Pretend to be something you aren't
  - Fake web server, fake DNS server, etc.
- Email address spoofing
  - The sending address of an email isn't really the sender
- Man-in-the-middle attacks
  - The person in the middle of the conversation pretends to be both endpoints
- Caller ID spoofing
  - The incoming call information is completely fake

DNS Poisoning
- Modify the DNS server
- Modify the client host file
- Send a fake response to a valid DNS request

Pharming
- Redirection to a bogus site
- Combines farming with phishing
  - Farming - Harvest large groups of people
  - Phishing - Collect access credentials
- Difficult for anti-malware software to stop
  - Everything appears legitimate to the user

Spam
- Unsolicited email, traditionally for advertising
- Can also be used to spread trojans/botnets

Spim
- Spam over IM
- Links in IM can be malicious

Spit
- Spam over internet telephony
- VoIP providers have made this difficult to practically implement

Stopping Spam
- White list to only allow known senders
- Black list to remove the bad senders
- Bayesian filtering can filter based on certain words/phrases
- Cloud-based spam services check email before it arrives

Phishing
- Social engineering with a touch of spoofing
- Often delivered by spam, IM, etc.
- Don't be fooled, check the URL
- Vishing is done over the phone
  - Fake security checks or bank updates

Spear Phishing
- More believable phishing with inside information
- Spear phishing the CEO is "whaling"

Xmas Tree Attack
- Send a carefully crafted packet to a host
- URG, PUSH, and FIN are set - 00101001
- Lit up "like a Christmas tree"
- May slow down the remote device (DoS)
- Easy to see this attack with an IPS
- Most modern devices will drop these packets

Privilege Escalation
- Gain higher-level access to a system
  - Exploit a vulnerability, might be a bug or design flaw
- Higher-level access means more capabilities
  - This commonly is the highest-level access
- These are high-priority vulnerability patches
  - You want to get these holes closed very quickly
  - Any user can be an administrator
- Horizontal privilege escalation
  - User A can access user B resources

Mitigating privilege escalation
- Patch quickly - Fix the vulnerability
- Updated anti-virus/anti-malware software
- Data Execution Prevention
- Address space randomization
  - Prevent a buffer overrun at a known memory address

Insider Threats
- We give people a lot of access
  - This is why we have the concept of least privilege
- You have more access than others by entering the building
- Lock away your documents
- Harms your organization's reputation
- Can cause a critical system distruption
- May include loss of confidential or proprietary information

Transitive attacks
- A trusts B, B trusts C, therefore A trusts C
  - This is not always the case in real life
  - Many times the case in network security
- Little control over the transitive
  - Common to trust nobody
- Firewalls often separate business partners
  - Firewalls can only stop so many things
  - You can't stop all access from your business partner

Client-side attacks
- Servers are more secure than ever
- Attack the client - Bad programming makes it easier
- Browsers, media players, office applications, email clients
  - A single insecurity can reveal all information
- Keep operating system and applications updated
  - A single vulnerability can own a computer

Attack Types (continued)

Password Attacks
- Brute force - Guess the password, calculate the hash
- Dictionary attack - Use common words as passwords
- Hybrid attack - Combine brute force and dictionary attacks
- Birthday attack - The same hash value for two plaintexts
- Rainbow tables - An optimized, pre-built set of hashes

Watering Hole Attack
- Determine which website the victim group uses
  - Educated guess - Local coffee shop, industry-related sites
- Infect one of these third-party sites
  - Site vulnerability, email attachments
- Infect all visitors, even if you're just looking for specific victims

URL Hijacking
- Typosquatting / brandjacking
  - Take advantage of poor spelling
- Outright misspelling
  - professormesser.com vs. professermesser.com
- A typing error
  - professormeser.com
- A different phrase
  - professormessers.com
- Different top-level domain
  - professormesser.org

Social Engineering Attacks

Shoulder Surfing
- You have access to important information, and people want it
- This is surprisingly easy
- Airports / flights, coffee shops
- Surf from afar with binoculars / telescopes
- Webcam monitoring

Preventing Shoulder Surfing
- Control your output
- Be aware of your surroundings
- Use privacy filters

Dumpster Diving
- Important information can be thrown out with the trash
- Easily gather details that can be used for a different attack
- Secure your garbage with a fence and lock
- Shred/destroy important documents

Tailgating
- Using someone else to gain access to a building
- Blend in with clothing
- Once inside, there's little to stop you
- Most security stops at the border

Watching for Tailgating
- Have a security policy for visitors
- One scan, one person
- Force a single entry with a mantrap / airlock
- Don't be afraid to ask when you see a stranger

Impersonation
- Pretend to be someone you aren't
- Use some of those details you got from the dumpster
- You can trust me, I'm with your help desk

Protecting against Impersonation
- Never volunteer information
- Don't disclose personal details
- Always verify before revealing info

Computer Hoaxes
- A threat that doesn't actually exist, but SEEMS real
- Still often consume lots of resources
  - Forwarded emailst, printed memorandums, wasted time
- Often an email or social network post
- A hoax about a virus can waste as much time as a regular virus

Stopping the Whale Hunts
- It's difficult to identify whaling with traditional security devices
  - Passes through the firewall and IPS
- Difficult to train
- Consider using practical exercises

Effective Social Engineering
- Constantly changing
  - You never know what they'll use next
- May involve multiple people
  - And multiple organizations
  - There are ties connecting many organizations
- May be in person or electronic
  - Phone calls from aggressive "customers"
  - Emailed funeral notifications of a friend or associate

Wireless Attacks

Rogue Access Points
- A significant potential backdoor
- Very easy to plug in a wireless AP
- Schedule a periodic wireless survey
- Consider using 802.1X (Network Access Control)

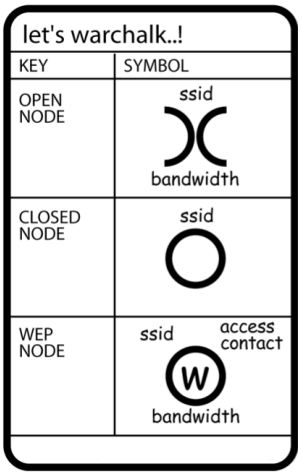
Evil Twins
- Buy a wireless access point
- Configure it exactly the same way as an existing network
- Same SSID and security settings
- May not require the same physical location
- Use HTTPS and a VPN to help mitigate

Wireless Interference
- Radio waves can be disrupted
- Intentional jamming or disruption of wireless signals is illegal in the United States (and elsewhere)
- Degrades or completely denies service
- May be used in conjunction with a wireless "evil twin"

Combating Interference
- Stop the offending station at the source
- May require additional monitoring equipment like a spectrum analyzer
- Boost the power of existing access points
- Try different frequencies

Wardriving
- Combine WiFi monitoring and a GPS
- Gather a huge amount of intel in a short period of time
- All of this is free with tools like Kismet, inSSIDer
- You can also use Warflying, warbiking

Warchalking
- Historical footnote to 802.11 wireless networking
- Created in June 2002, publicized by Matt Jones
- If you find a node, let someone else know
- By the time this was a big problem, it wasn't a problem anymore



Bluejacking
- Sending of unsolicited messages to another device via Bluetooth
- Typical functional distance is about 10 meters
- Bluejack with an address book object, instead of contact name a message is written
  - "You are Bluejacked! Add to contacts?"
- Third-party software may also be used, Blooover, Bluesniff

Bluesnarfing
- A rare attack that takes advantage of a vulnerability
- Access a Bluetooth-enabled device and transfer data
- Exploited through security weakenesses
  - Must be fixed with a patch
- If you know the file, you can download it without authentication

Wireless Initialization Vector Attacks
- IV is an extra bit of data thrown in to change the encryption stream
- The IV changes each time data is sent (ideally)
- With 802.11 WEP, the IV is passed along with the encrypted data
- The other side reverses the process

WEP IV
- No key management, everyone usually has the same key
- The WEP IV is 24-bits long - relatively small
  - 16,777,216 possible RC4 cypher streams for a given WEP key
- IV values eventually are reused
- Some "weak" IVs don't properly provide for good encryption, and makes it easy to discover the key
- The bad guys will inject frames to intentionally duplicate IVs and make key identification easier

Wireless Packet Analysis
- Most information over the network is "in the clear"
- Relatively difficult to capture data over wired networks
- Wireless networks are incredibly easy to monitor
- Some network drivers won't capture wireless information
- Free capture software - http://www.wireshark.org

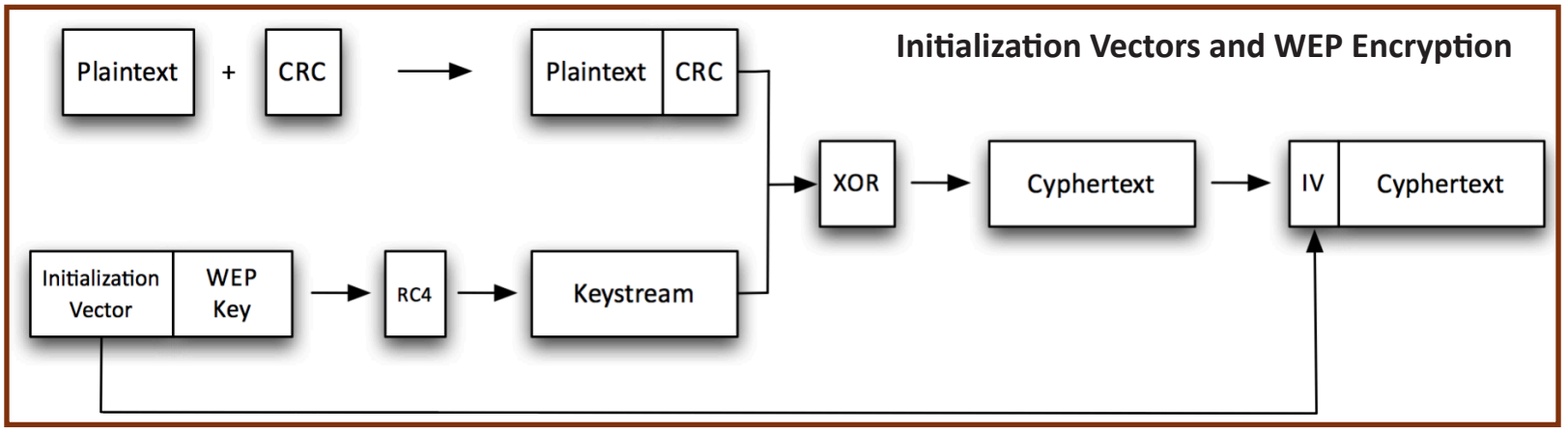
Protecting against packet analysis
- Use WPA2 encryption on your wireless access point
- Use encryption for authentication
- Use end-to-end VPN
- Use encrypted proxy services and virtual tunnel networks

Near Field Communication (NFC)
- Two-way wireless communication
- Payment systems, i.e., Google wallet and MasterCard
- Bootstrap for other wireless - NFC helps with Bluetooth pairing
- Access token, identity "card" - Short range with encryption

NFC Security Concerns
- Remote capture - It's a wireless network
- Frequency jamming - Denial of service
- Relay attack - Man in the middle
- Loss of RFC device control - Stolen/lost phone

WPA Attacks
- WPA-Personal / WPA-PSK
  - WPA with a pre-shared key
  - Everyone uses the same 256-bit key
  - The only way in is a brute force / dictionary attack
  - Some cloud-based services already have the hashes
  - Use a complex set of letters and numbers / Avoid words
- WPA-Enterprise / WPA-802.1X
  - Authenticates users individually with an authentication server
  - No practical attacks

WPS Attacks
- PIN is an eight-digit number
  - Really seven digits and a checksum
  - Seven digits, 10,000,000 possible combinations
- The WPS process validates each half of the PIN
  - First half, 4 digits. Second half, 3 digits.
  - First half, 10,000 possibilities. Second half, 1,000 possibilities
- It takes about four hours to go through all of them
  - Most devices never considered a lockout function



Application Attack Types

Cross-site Scripting (XSS)
- Called cross-site because of browser security flaws
- Information from one site can be shared with another
- One of the most common vulnerabilities
- Used by malware that uses JavaScript vulnerabilities

Non-persistent (reflected) XSS attack
- Web site allows scripts to run in user input /search box
- Bad guy may email a link
  - Email link runs a script that sends credentials/session IDs/cookies to the bad guy
  - Script embedded in URL executes in the victim's browser, as if it came from the server
  - Bad guys use credentials/session IDs/cookies to steal victim's information without their knowledge

Persistent (stored) XSS attack
- Bad guy posts a message to a social network that includes a malicious payload (it's now "persistent")
  - Everyone gets the payload
  - No specific target
  - For social networking, this can spread quickly
- Everyone who views the message can have it posted to their page, where someone else can view it and propagate it further...

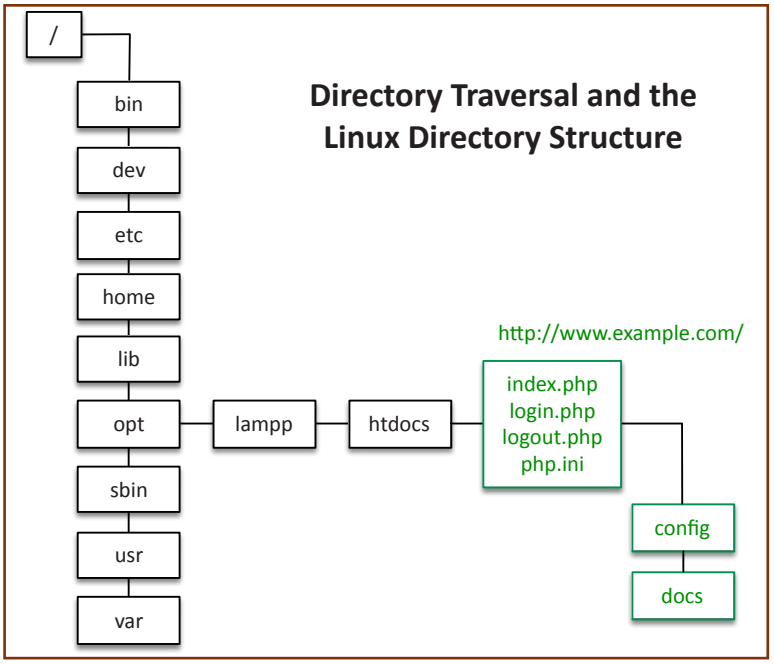
Protecting Against XSS
- Be careful when clicking untrusted links
- Consider disabling JavaScript, or control with an extension
- Keep your browser and applications updated
- Keep your web server applications updated

Code Injection
- Adding information into a data stream
- Applications should be developed to properly handle input and output
- Used with many different data types
  - HTML, SQL, XML, LDAP, etc.

SQL (Structured Query Language) Injection
- The most common relational database management system language
- SQL Injection modifies SQL requests in the browser
- The application should be written to prevent this

XML Injection and LDAP Injection
- XML - Extensible Markup Language
- XML injection modifies XML requests
  - A good application will validate all input
- LDAP - Lightweight Directory Access Protocol
- LDAP injection modifies LDAP requests to manipulate application results

Directory Traversal
- A misconfigured server allows inappropriate access
- Command injection can be dangerous when this happens
  - Run unauthorized commands from your browser
- Combine with directory traversal for really scary results



Zero-day Attacks
- Many applications have undiscovered vulnerabilities
- Someone is working hard to find the next big vulnerability
- A zero-day vulnerability has not been detected or published
- Zero-day exploits are increasingly common
- Common Vulnerabilities and Exposures (CVE) - http://cve.mitre.org/

Browser Cookies and Session IDs
- Cookies contain browser information stored on your computer
  - Used for tracking, personalization, session management
- Not executable, not generally a security risk
- Could be considered be a privacy risk
- Session IDs are often stored in the cookie
- Used with cookies to masquerade as another person

Buffer Overflows
- Overwriting a buffer of memory
- Spills over into other memory areas
- Developers need to perform bounds checking
- The bad guys spend a lot of time looking for openings
- A really useful buffer overflow is repeatable

Integer Overflow
- Usually has a fixed boundary
- Vulnerable software may allow an integer to go out of bounds
- This integer may allocate a memory location for a buffer
  - The buffer will now be too small, and overflow may occur

Variable A and B before buffer overflow

Variable Name	A								B	
Value	[null string]								1979	
Hex Value	00	00	00	00	00	00	00	00	07	BB

Overflowing variable A changes variable B

Variable Name	A								B	
Value	'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	25856	
Hex Value	65	78	63	65	73	73	69	76	65	00

Application Attack Types (continued)

Locally Shared Objects
- Also called Flash Cookies
  - Used by Adobe Flash Player to store data
  - Information is saved on the user's computer
  - On by default
- Applies to all browsers
  - Data is stored in a common directory
- Can only be read by the domain that created the LSO
  - www.example.com can only be read by www.example.com
  - Unless specifically passed to another domain

LSO and Privacy Concerns
- You can store anything in the Flash cookie
- Many web sites use Flash cookies
- Class-action suits have been filed regarding LSOs
  - Personal information has been given to third-parties
- Some countries require knowledge and consent

Malicious Add-ons and Attachments
- Attachments may be files sent via email
  - All attachments should be considered a security risk
- Add-ons extend your browser functionality
  - Add-ons tend to be more trusted

Arbitrary and Remote Code Execution
- Arbitrary code execution - The attacker runs whatever they want
- An attacker takes over a process
  - The original executable is vulnerable to this attack
- No elevated rights needed for many attacks
  - Infect with malware or adware
- Remote code execution
  - Attack a machine from a remote device
  - Extremely dangerous vulnerability

Mitigation and Deterrent Techniques

Monitoring System Logs
- Huge source of detailed network information
- Routers, switches, firewalls, IDS/IPS, anti-virus scanners, applications, authentications, etc.
- Contain data on servers, applications, security

Event Logs
- Details of normal activity
- Not remarkably useful in the moment, very useful after the fact
- Huge storage requirements
- Logs from everything - Servers, routers, switches, firewalls

Audit Logs
- Changes must be controlled
- Can recognize legitimate activity
  - Firewall policy change, file permission update
- Can recognize unapproved activity, unapproved changes
- Not as many logs as event log, but perhaps more important

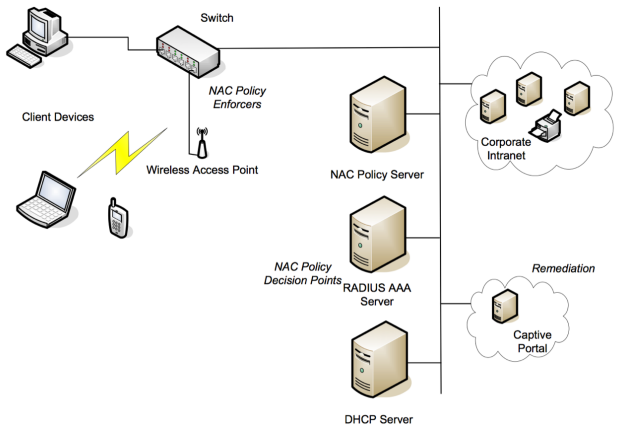
Access Logs
- Many different instances of access
  - Files, VPN connection, partners, customers
- Many different formats - Servers, application logs, etc.
- Important to know who's coming in and out, and who is failing
- Automation can limit the attack vector
- Very useful when rebuilding after an attack

Security Logs
- Focused on security-related events
- Very specific events
  - Not necessarily useful to the rest of the organization
- Many diverse devices
  - Firewall, VPN concentrator, IPS, content filter, authentication server, router, switch, email gateway, anti-virus manager, etc.
- Often requires it's own logging strategy

Operating System Hardening
- Increase the security of your operating system
- Constant maintenance to patch vulnerabilities
- One configuration error can inadvertently create an opening
- Plan a regular preventive maintenance cycle

MAC Limiting and Filtering
- Media Access Control - The physical address of your interface
- Collect and filter the MAC address of all devices
- MAC addresses are easily spoofed
- Don't rely on this for security

802.1X



Physical Port Security
- This is a good best-practice
- Requires additional maintenance and constant vigilance
- Plan on periodic reviews using the switch management console

Rogue Machine Detection
- Find devices that should not be on the network and remove them
- Visual audit - Check ports and switches for incursion
- Network mapping - Automated functions for finding devices
- Wireless audits - Walk around and find rogue access points
- Network Access Control (NAC)
  - Require authentication before gaining access to the network

Security Posture
- Initial Baseline Configuration
  - Determine the minimum level of protection required
- Continuous Security Monitoring
  - New threats are announced every day
  - Systems are constantly modified and updated
- Remediation network
  - Access may be based on the missing security
  - Access allowed once the device is back to full security posture

Mitigation and Deterrent Techniques (continued)

Alarms and Alerts
- Every device contains information
- Define metrics to monitor (throughput, authentications, etc.)
- Define thresholds per metric - Up/down, Percentage, Exact value
- Disposition - Email, SMS

Trends
- Identify details that would be otherwise invisible
- Monitoring intervals and reporting timeframes
- You're collecting a LOT of data - age it out as you go
- Focus on security metrics - Malware activity, patch failures, increase in bandwidth, etc.

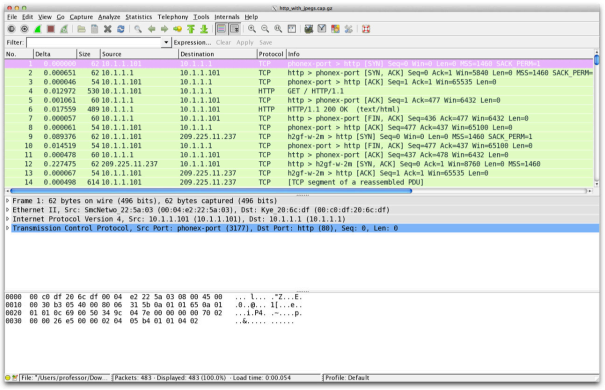
Security Threats and Vulnerabilities

Vulnerability Scanning
- Vulnerabilities are identified every day
- National Vulnerability Database (http://nvd.nist.gov/)
- Applications, operating systems, services
- Scan a device to determine susceptibility to a known vulnerability
- Can be quite invasive
- Scan general OS, web servers, application, database servers

Interpreting Vulnerability Scans
- Scanners aren't perfect
- Network-level challenges with firewalls
- Device-level challenges with OS changes, patch updates, application versions

Passive vs. active tools
- Passive tools
  - No interaction
  - Gather information external to the device
  - Packet captures
- Active tools
  - The device can see you looking
  - Vulnerability scanners, honeypots, port scanners, banner grabbing

Protocol Analyzer
- Capture and display network traffic, Packet by packet
- Wireshark, a popular open-source option
- Valuable vulnerability recon - Encrypt your traffic



Vulnerability Scanners
- Application scanners identify vulnerabilities in web servers, database servers, etc.
- OS scanners identify operating system vulnerabilities for Windows, Linux, Mac OS, etc.

Honeypots and Honeynets
- Attract the bad guys and trap them there
- Makes for interesting recon
- Honeypots
  - Single-use/single-system traps
- Honeynets
  - More than one honeypot on a network

Port scanners
- Identify open ports on a system
- Identify firewalls and packet filters
- Identify operating systems and services
- Based on simple packet requests and responses
- Identify applications without authenticating

Banner Grabbing
- Applications can be chatty
- The banner is always there
- Capture it with telnet or an automated tool

Quantitative Risk Assessment
- Assign a dollar value to risk
- Single Loss Expectancy (SLE)
  - How much loss for one event?
- Annual Loss Expectancy
  - SLE x Annual Rate of Occurrence (ARO)

Qualitative Risk Assessment
- Identify significant risk factors
- Ask opinions about the significance
- Display visually with traffic light grid or similar method

Vulnerability Assessment
- Actively scan a network in search of known vulnerabilities
- Usually an automated process
- For unknown vulnerabilities, consider input validation/fuzzing

Assessment Techniques
- Baseline Reporting
- Determine risk
- Determine which metrics and resources to monitor
- Changes might indicate security concern
- The baseline is constantly changing

Code Review
- Audit your in-house applications
- Examine the source code
- Test for input validation, injection attacks, etc.

Design Review
- High-level application review
- How many ways can a user interact with the application?
- Consider the different attack surfaces
- Check form fields, APIs, etc.
- Keep the attack surface small

Architecture Review
- Review the database engine, Web server, browser type
- Consider confidentiality, integrity and availability
- Not all servers provide the same security posture

Penetration Test and Vulnerability Scanning

Penetration Testing (Pentest)
- Simulate an attack
- Similar to vulnerability scanning, except we actually try to exploit the vulnerabilities

Verify a threat exists
- Stay up-to-date
- Reference the National Institute of Standards and Technology National Vulnerability Database
  - http://nvd.nist.gov
- Perform regular vulnerability scans

Bypass Security Controls
- Force your way in
- People in the organization may bypass security controls

Actively Test Security Controls
- Attempt to circumvent the same controls as the bad guys
- Test with different techniques
- This should represent what the bad guys see

Exploiting Vulnerabilities
- Try to break into the system
  - This might cause a denial of service or loss of data
  - Buffer overflows can cause instability
- You may need to try many different vulnerability types
  - Password brute-force
  - Social engineering
  - Database injections
  - Buffer overflows
- You'll only be sure you're vulnerable if you can successfully exploit a system
- If you can get through, the bad guys can get through

Black Box, White Box, and Grey Box
- Black box - A "blind" test
  - The pentester knows nothing about the systems
- White box
  - Full disclosure - The pentester knows everything
- Grey box
  - A mix of black and white
  - Focus on certain systems or applications

Vulnerability Scanning
- A passive test, unlike a penetration test
- May include port scanning
- Test from both the outside and inside
- Gather as much information as possible

Scan Types
- Non-intrusive scans
  - Gather information, don't try to exploit a vulnerability
- Intrusive scans
  - You'll try out the vulnerability to see if it works
- Non-credentialed scans
  - The scanner can't login to the remote device
- Credentialed scan
  - You're a normal user, emulates an insider attack

Identify Vulnerabilities
- The scanner looks for many vulnerability types
- The vulnerabilities can be cross-referenced online
- Some vulnerabilities cannot be definitively identified

Vulnerability Scan Results
- Many results can be identified:
  - Lack of security controls
  - No firewall
  - No anti-virus
  - No anti-spyware
  - Misconfigurations
  - Open shares
  - Guest access
  - Real vulnerabilities

False positives
- A vulnerability is identified that doesn't really exist
- This is different than a low-severity vulnerability
- It's real, but it may not be your highest priority

False negatives
- A vulnerability exists, but you didn't detect it
- Update to the latest signatures
- Work with the vulnerability detection manufacturer
  - They may need to update their signatures

Application Security Controls and Techniques

Fuzzing
- Send random input to an application
- Fault-injecting, robustness testing, syntax testing, etc.
- Looking for something out of the ordinary, such as an application crash, server error, exception
- Many different fuzzing utilities and options
- Fuzzing is time and resource heavy
- Many fuzzing engines use high-probability tests

Secure Coding Concepts
- There's a balance between time and quality
- Programming with security in mind is often secondary
- The Quality Assurance (QA) process tests applications
- Vulnerabilities will eventually be found

Input Validation
- Validate actual input and expected output
- Document all input methods (forms, fields, type)
- The fuzzers will find what you missed

XSS and XSRF Prevention
- Cross-site scripting (XSS)
  - Check the input for embedded scripts
  - Validate the input prior to storing
- Cross-site request forgery (XSRF)
  - One-click attack / session riding
  - Authentications should be protected and/or encrypted

Error and Exception Handling
- What happens when an error occurs?
  - Network connection fails, server hangs, database unavailable
  - Think of every possible problem
- Mishandled exceptions can allow execution of code

Cross-site Scripting (XSS)
- Called cross-site because of browser security flaws
- Information from one site can be shared with another
- One of the most common vulnerabilities
- Used by malware that uses JavaScript vulnerabilities

Non-persistent (reflected) XSS attack
- Web site allows scripts to run in user input /search box
- Bad guy may email a link
  - Email link runs a script that sends credentials/session IDs/cookies to the bad guy
  - Script embedded in URL executes in the victim's browser, as if it came from the server
  - Bad guys use credentials/session IDs/cookies to steal victim's information without their knowledge

Persistent (stored) XSS attack
- Bad guy posts a message to a social network that includes a malicious payload (it's now "persistent")
  - Everyone gets the payload
  - No specific target
  - For social networking, this can spread quickly
- Everyone who views the message can have it posted to their page, where someone else can view it and propagate it further...

Protecting Against XSS
- Be careful when clicking untrusted links
- Consider disabling JavaScript, or control with an extension
- Keep your browser and applications updated
- Keep your web server applications updated

Application Configuration Baseline
- Determine a security baseline for every application
- Monitor the baseline over time
- Perform scheduled scans
- Once-a-month security patches and service packs
- May require security testing after major updates

Application Hardening
- Update the operating system
- Apply security patches and service packs
- Update application software
- Restrict user accounts to "least privilege" access
- Restrict additional software installations

Application Patch Management
- May provide additional features
- Patches may fix bugs
- Close any open security holes

Updating Operating Systems
- Use Windows Update for client-initiated updates
- Centralize patch management with Windows Server Update Services (WSUS)
- Mac OS - update from the Apple menu / Software Update
- Linux - update using rpm, yum, apt-get, software update GUI

The Patch Management Challenge
- A bug fix might introduce others
- Updating one application might break another
- Security updates are important
- Don't forget your security check after updating, based on your application security baseline

SQL Databases
- Keep important information centralized
  - In a format that allows for easy retrieval
- Relational Database Management Systems (RDBMS)
  - Data is stored in a table
  - Each table has records/rows
  - Each table is like a big spreadsheet
- Structured Query Language (SQL)
  - Standard programming language for database interaction
- Very common method of storing data

NoSQL Databases
- Not Only SQL
  - Not SQL, not relational
- A good choice for large datasets
  - Scales very large
- Can analyze very large unstructured data sets
  - Big data
- Grab as much data as you can and put it into a database
  - There might be relationships between the data, or perhaps not
  - The database needs to be able to handle anything

Categories of NoSQL Databases
- Key-value store
  - Relies on a hash table to locate and represent data
- Column family store
  - Large data stores can reference multiple columns with a single key
- Document database
  - Similar to key-value stores
  - Contains documents that are collections of other key-value collections
- Graph database
  - Instead of a spreadsheet, use nodes, node properties, and the relationship between the nodes

Validating Data
- Attack an application through the user input
  - Provide data the application isn't expecting
  - Unexpected results may occur
- SQL injection
  - Gain access to the database
- Filenames
  - Traverse the file system
- Perform extensive tests before releasing app
  - Fuzzing or random input testing

Validation Points
- Server-side validation
  - All checks occur on the server
  - Helps protect against malicious users
    - Bad guys may not even be using your interface
- Client-side validation
  - The end-user's app makes the validation decisions
  - Can filter legitimate input from genuine users
  - May provide additional speed to the user
- Use both
  - But especially server-side validation

Mobile Device Security

Mobile Device Management
- 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 remote device
  - The entire device or a “partition”
- Manage access control
  - Force screen locks and PINs on these single user devices

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 trival
  - Uses a lot of CPU cycles
- Don’t lose or forget your password!
  - There’s no recovery

Remote Wipe / Sanitation
- Remove all data from your mobile device
  - Even if you have no idea where it is
- Connect and wipe from the web
  - Nuke it from anywhere
- Need to plan for this
  - Configure your mobile device now

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 agressive lockout timers
  - Completely lock the phone

GPS Tracking
- Precise tracking details - Tracks within feet
- Can be used for good - Find your phone
- Can be used for bad - Find you
- Most phones provide an option to disable
  - Limits functionality of the phones

Application Control and Storage Segmentation
- An MDM can control exactly what’s loaded
  - Only approved corporate applications
- Unapproved applications are restricted or removed
  - The MDM has complete control
- Some MDM software segments corporate data
  - A separate area of the mobile device
  - Run personal and corporate without conflict
- Some devices support removable storage
  - Control where organization’s data is stored
- Individual and unused features can also be disabled
  - Bluetooth, video camera, etc.

Asset Tracking and Inventory Control
- Mobile devices are…mobile
  - They could be anywhere in the world
- Some organizations purchase phones for their users
  - Doesn’t change the asset tracking process
- Location services becomes important
  - You know where every device is at all times
  - Or the last time they checked-in
- Security policies should include monitoring details
  - Privacy concerns differ across countries

Encryption and key management
- Encrypted data is important to mobile devices
  - Keep your information safe as it moves around
- Is information encrypted when stored on the device?
  - Every application does this differently
- Data across the network
  - Use the device APIs to send traffic via SSL
- SSL requires a stored group of trusted Certificate Authorities (CA)
  - Locally-created CA certificates can be added through an MDM

Credential Managment
- Usernames and passwords
  - Always separated from the application code
- Credential details are almost always server-based
  - Easier to protect and manage
- Credentials are usually communicated over SSL
  - Sometimes the app doesn’t actually encrypt anything!
- Use a transitive trust for authentication
  - Login with Facebook, Google, etc.

Geo-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

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

User Acceptance and Adherence to Corporate Policies
- Corporate control of a personal device
- Users must accept the integration of work onto the mobile device
- Mobile Device Managers (MDMs) will be used
- Specific security controls ensure adherence to corporate policies
- May be a different acceptable use policy (AUP) for BYOD devices
- A personal device, but used for business - Which policy wins?

Mobile Device Security (continued)

Architecture and infrastructure considerations
- Not all devices can be reasonably managed
  - The organization may create a list of approved devices
- All devices must be managed through the MDM
  - The device manager may have limitations on the type and number of devices
- MDMs must be purchased, installed, etc.
  - Training costs, ongoing management costs
- May require specific connectivity to the Internet
  - The MDM must talk to the mobile devices directly

Support ownership and on/off-boarding
- The organization now supports the device
  - If lost, the first call is to the corporate help desk
  - Not the wireless provider
- Corporate office needs to wipe data
  - Or selectively remove the organization's informationv
- On-boarding and off-boarding is more involved
  - Carve out the organization's section of the device
  - Remove just the organization's data
  - I would completely nuke and rebuild

Patch and Anti-virus Management
- Mobile devices are used everywhere
  - In the building, out of the building
- New applications are installed all the time
  - With the potential for malware and viruses each time
- Some patches may break other features
  - Or important corporate applications
- On-device anti-virus may be required
  - Manage through the MDM

Data Ownership and Privacy
- The device belongs to a person
  - Some of the data belongs to the organization
  - Some of the data is very private
- Use policies to determine data ownership
  - Document and communicate detailed security policy
- Use technology to determine data ownership
  - Storage segmentation can build walls around employer data
  - Separate apps, separate data in the enterprise "box"

On-board Camera and Video
- A corporate and social challenge
  - Privacy concerns, industrial espionage
- Some policies restrict the use of the camera
  - Always available or always disabled
- Some MDMs allow for geo-fencing
  - Restrict or allow features when in a particular area (The camera might only work when outside the office)

Forensics and Legal Concerns
- Post-attack actions
  - What forensic processes are followed?
- With a desktop, the entire device is quarantined
  - The organization may not own the mobile device
- The mobile device contains personal data
  - The forensics process may need to look at all information
- Does the organization have a legal right to the device/data?
  - Does the user have a legal requirement of privacy to their data?

Establishing Host Security

Customizing OS Securtity Settings
- User rights - Access to files and groups
- Log settings - Event log detail and log forwarding
- File permissions
  - Access to certain files, completely restrict others
- Registry permissions - Not all registry hives should be accessible
- Account policies - What each user can and cannot do

Anti-Virus
- Millions of virus signatures are known
- Always install an anti-virus application
- Always keep the signatures current!
- No anti-virus application can stop everything

Anti-Spyware
- Malware that watches you and reports back
- May track browsing activity, keylogs, username/password information
- Always use an anti-spyware application

Anti-Spam
- Unsolicited emails (buy my stuff)
- Phishing attempts to obtain your username and password
- Many email clients include anti-spam technology
- Your ISP may include this in the cloud

Pop-up Blockers
- Messages appear in separate windows in your browser
- Became popular as an advertising method
- Malware is especially good at popping windows
- Legitimate applications may use pop-up windows

Host-based Firewalls
- Protect against others on the network
- Can restrict access to your personal computer
- Protect wherever you go
- Important for laptops and mobile devices
- Restricts by application and network port numbers

Patch Management
- Incredibly important
- Provides system stability
- May include security fixes and service packs
- Provides emergency out-of-band updates
- Protect against 0-day and important security discoveries

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

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

Trusted OS
- Evaluation Assurance Levels
- Common Criteria for Information Technology Security Evaluation
  - Also called Common Criteria (or CC)
  - Very 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

Host-Based Firewalls
- "Personal" firewalls
  - More than personal these days
- Included in many operating systems
  - 3rd-party solutions also available
- Stops unauthorized network access
  - "Stateful" firewall
  - Blocks traffic by application
- Windows Firewall
  - Filters traffic by port number and application

Host-Based Intrusion Prevention
- Started as a separate application
  - Now integrated into many "endpoint" products
- Protect based on signatures
  - Constantly growing database
- Protect based on activity
  - Why are you modifying that file?

Cable Locks
- Temporary security
  - Connect your hardware to something solid
- Cable works almost anywhere, useful when mobile
- Most devices have a standard connector
  - Reinforced notch
- Not designed for long-term protection
  - Those cables are pretty thin

Safe
- Secure your important hardware and media
- Protection against fire and water
- Very heavy and difficult to steal
- Access must be carefully managed

Locking Cabinets
- Data center devices may be managed by different groups
- Responsibility lies with the owner
- Racks can have enclosed cabinets with locks
- Ventilation on front, back, top, and bottom

Host Software Baselining
- Security baselining
  - Determine what the application requires
  - Host resources, network connectivity, etc.
- Need to tighten down operating system
  - Host-based firewall
  - Application execution restrictions
  - Limit access to certain folders
- Useful for configuring external security devices
  - Firewall security policies
  - Allow or restrict application communication

Software on the Server
- Web server, cloud based
  - The application is centralized
- Other services may be using the same physical hardware
  - Difficult to completely secure and limit access
- Redundancy may be required
  - Protect against downtime
  - Denial of Service (DoS)
  - Hardware failures
  - Network outages

Virtualization
- One physical computer, many operating systems
  - Mac OS X, Windows 7, Linux, all at the same time!
- Separate OS, independent CPU, memory, network, etc.
- Host-based virtualization runs all OSes on your desktop

The Hypervisor
- The VMM (Virtual Machine Manager)
- Manages the virtual platform and guest operating systems
- May require a CPU that supports virtualization

Snapshots and Security
- Every guest is self-contained in a single file
- Virtual hosts can be versioned
  - Take snapshots at any point, revert instantly
  - Store multiple snapshots
- Easy to recover to a specific date and time
- Historical analysis - determine when a vulnerability was exploited

Host Availability / Elasticity
- Elasticity
  - Provide resources when demand requires it
  - Scale down when things are slow
- Host availability
  - New server deployed with a few mouse clicks
- Virtualization integrates a layer of orchestration
  - Automate the deployment and movement of virtual hosts
- Servers can be added or moved to other data centers
  - All of the management systems follow the servers

Using Virtual Hosts for Security
- Virtualized hosts are perfect for spinning up a custom host
- Network scans, vulnerability scanning, penetration testing
- Sandboxing
  - Don't click that link! Don't launch that attachment!
  - Unless you're in a sandbox
- Individual sandboxes
  - Or centralized sandboxes for everyone

Ensuring Data Security

SAN Data Security
- The network is the SAN
  - You're in one place, the data is in another
- Physically secure SAN
  - Restricted physical access
  - Protected data center
  - Self-encrypting drives
- Encrypt data when it leaves the protected area
  - Network-to-network (switch-to-switch)
  - Backup tapes
  - Plan for encryption overhead in CPU and network use

Securing Big Data
- Massive datasets
  - Normal access controls may not apply
- Doesn't fit a "need to know" principle
  - You don't even know what's in there
  - An important part of big data is hunting for patterns
- Consider removing Personally Identifiable Information (PII)
  - Difficult to completely remove an individual's identification
- Difficult to audit every bit of information accessed
  - Log just the queries
  - Implement Data Loss Prevention (DLP) techniques

Full-Disk Encryption
- Serious data protection - Every bit and byte is encrypted
- Perfect for mobile devices - But not exclusive to laptops
- Built-in protection - BitLocker
- Commercial and open-source options - PGP, TrueCrypt
- Key management is incredibly important
  - Lose the key, lose your data

Database Encryption
- Relatively impractical to encrypt an entire database
  - Huge files, lots of access
- Encryption based on the Database Management System (DBMS)
  - Different capabilities across different software platforms
- Individual columns/fields are usually encrypted
  - Don't encrypt your key fields!

Individual File Encryption
- Many different options
  - Built-in to the OS
  - 3rd-party applications
- Some files are encrypted others are not
  - Pick and choose your security
  - And your resource management
- Many of those still require key management
  - Backup your keys, protect your keys

Removable Media Encryption
- Big concern
  - Where's my USB drive?
- Administrative controls over removable media
  - Require encryption
- Again with the key management
  - This can be automated in many operating systems
- No USB storage at all
  - An extreme case

Mobile Devices
- Practically all mobile devices encrypt user data
  - The key is on the device
- Email and apps using "Data Protection" are encrypted in iOS
  - The key is based on the passcode
  - Even if stolen, you can get the data
- Some information may not be encrypted in iOS
- On Android, configure encryption in Settings > Security
  - Full-disk encryption, the key is based on the passcode

Trusted Platform Module (TPM)
- A specification for cryptographic functions
- Cryptographic processor with random number generator, key generators
- Persistent memory
  - Comes with unique keys burned in during production
- Versatile memory
  - Storage keys, hardware configuration information
- Password protected

Hardware Security Module (HSM)
- High-end cryptographic hardware
  - Plug-in card or separate hardware device
- Key backup in secured storage
- Cryptographic accelerators for offloading CPU overhead
- Used in large environments

USB Encryption
- Hardware-based AES encryption as part of the drive
- Includes trusted browser, identity software
- Can be used as secure tokens with two-factor authentication and single sign-on
- Remote management included to unlock or reset remotely

Hard Drive Encryption
- Encrypt storage drive data with hardware
- Integrate with USB key
- Cleartext goes in, cipher comes out
- High speed, strong encryption

Data In-Transit
- Data transmitted over the network
  - Also called data in-motion
- Not much protection as it travels
  - Many different switches, routers, devices
- Provide transport encryption
  - TLS (Transport Layer Security), IPsec (Internet Protocol Security)

Data At-Rest
- The data is on a storage device
- Encrypt the data
  - Whole disk encryption, database encryption
  - File- or folder-level encryption
- Apply permissions
  - Access control lists - only authorized users can access the data

Data In-Use
- The data is in memory
  - System RAM, CPU registers and cache
- The data is almost always decrypted
  - Otherwise, you couldn't do anything with it
- The bad guys can pick the decrypted information out of RAM

Ensuring Data Security (continued)

Access Control Lists
- ACLs
  - Permissions associated with an object
  - Used in file systems, network devices, operating systems, and more
- List the permissions
  - Bob can read files
  - Fred can access the network
  - James can access network 192.168.1.0/24 using
  - tcp ports 80, 443, and 8088
- Many operating systems use ACLs to provide access to files
- A trustee and the access rights allowed

Data Wiping
- Remote removal of data
  - The administrator can delete all or part of live data
- Retiring hardware
  - Hard drives contain a lot of information
  - Overwrite all disk data before disposing
- May be based around device loss or employee off-boarding
  - The organization controls the location of data at all times

Disposing of Data
- Some information cannot be disposed of
  - Legal requirements for maintaining information
- Some information is destroyed to make room for more
  - Archived data, especially with high storage costs
- Personal data may have a very short life
  - Only store for however long as is necessary
- Sensitive information may be destroyed to control distribution
  - Keep the information out of the hands of others

Data Retention
- Keep files that change frequently for version control
  - Files change often - Keep at least a week, perhaps more
- Recover from virus infection
  - Infection may not be identified immediately
  - May need to retain 30 days of backups
- Consider legal requirements for data retention
  - Email storage may be required over years
  - Some industries must legally store certain data types
  - Different data types have different storage requirements

Mitigating Security Risks

Static Environments
- User can't change very much, unlike a PC
- Very useful for security - Easier to protect and defend
- Embedded systems
  - A computing system designed to
  - perform a specific, dedicated function
  - Intravenous drip-rate meter, water treatment plant controls
- Even static environments can be updated
  - Firmware upgrades are common

SCADA and HVAC
- Supervisory Control and Data Acquisition System
  - Large-scale, multi-site Industrial Control Systems (ICS)
- Runs on normal PCs, manages equipment
  - Power generation, refining, manufacturing equipment
- Traditionally not built with security in mind
  - This has obviously been a problem these days
- Huge emphasis in securing all SCADA systems
  - Enormous improvements in a short time

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

In-Vehicle Computing Systems
- Huge amount of computing power in a car
  - Navigation, in-vehicle entertainment
- Engine electronics
  - Embedded technology for fuel consumption and engine functions
- Telemetry
  - Event data recorder "black box"
  - Acceleration, braking, position

Apple iOS
- Operating system for many different products
  - iPod, iPhone, iPad
- Closed operating system
  - Derived from Unix
- Apps available in the App Store
  - Developers must submit their apps for approval
  - Only one place to download applications
- Very closed environment
  - Security issues are relatively mitigated

Android
- Open Handset Alliance
  - Driven by Google
- A more open model than iOS
  - Open-source operating system
- A more open app distribution system
  - Completely distributed, no centralized store
- More susceptible to malware
  - Applications have limited access to user data
  - Unless the user allows it

Smart Televisions
- Connect TV, Hybrid TV
  - Combine a computer with a television
- Stream video/audio, video on demand, games, social networking, etc. - Video without an antenna
- Most use a Linux kernel
  - Security concerns associated with JavaScript, HTML5, Java, etc.
- Disable if features aren't needed
  - Office conference room, OTA-only

Mitigating Security Risks (continued)

Mainframes
- Legacy systems - Proprietary operating systems
- Still used for large-scale applications
  - Bulk data, transaction processing
- Very reliable and redundant
  - Can run interrupted for decades
- Not many mainframe-specific attacks exist
  - A unique OS with relatively few installations
- Attacks tend to be from the inside
  - Very specialized, attacking specific data sources

Game Consoles
- Very similar to a PC - Specific hardware and a purpose-built OS
- Xbox and PlayStation - Windows and Linux
- Large storage and CPU capacity - Perfect to use as a server
- Rooting or jailbreaking - Gain access to the hardware and/or the OS
- Network-centric - Keep away from the corporate network

Security Layers and Control Redundancy
- Layered security
  - Defense-in-depth - You need more than just one type of security
- The security controls should be diverse
  - If you get over one hurdle, there's another one to stop you
- Avoid any single points of failure
  - Security also needs redundancy
  - Multiple firewalls, multiple IPS, multiple management systems

Network Segementation
- Separate logical sections of the organization
  - Internet, DMZ, storage, management, corporate, etc.
- Physical separation
  - Completely different infrastructure
- Logical separation
  - Firewall rules, based on zones or IP address ranges
- Specific policies for types of data per zone
  - No PII in the DMZ, no credit card information on the Internet

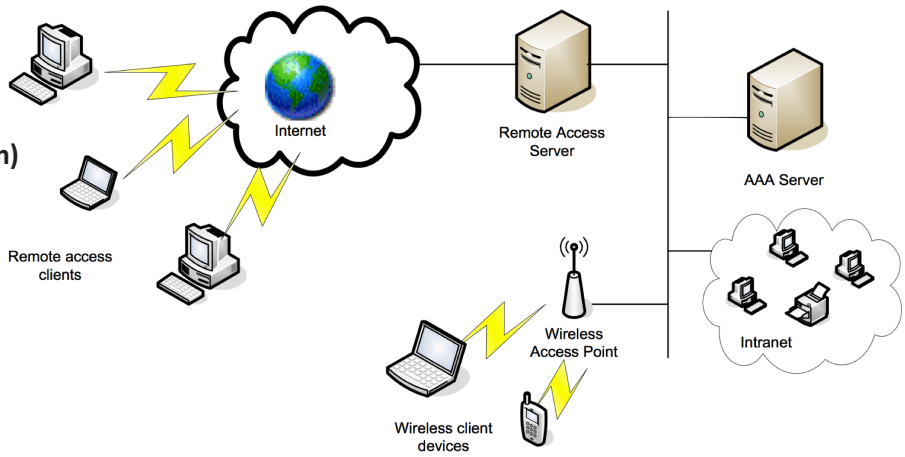
Wrappers and Application Firewalls
- TCP Wrapper
  - Puts a wrapper between the network and the service
  - Used ACLs to filter access to services
  - A very early form of application control
- Application firewalls - Filters traffic based on the application
  - Can provide very detailed application control
  - Can protect specialized applications

Firmware Version Control
- Embedded systems have relatively few updates
- Some embedded systems can't be updated easily
- Many embedded systems require manual updates
  - There's no automated process or external management
  - More time consuming
  - May be seen as less of a priority

Authentication Services

RADIUS (Remote Authentication Dial-in User Service)
- Authentication protocol for almost everything
- A very common AAA service
  - Modems, routers, switches, firewalls, etc.
- A common authentication method for 802.1X
- Secure authentication - sends passwords as a hash

TACACS (Terminal Access Controller Access-Control System)
- Remote authentication protocol, RFC 1492
- Created to control access to dial-up lines to ARPANET
- XTACACS (Extended TACACS)
  - A Cisco-created (proprietary) version of TACACS
  - Additional support for accounting and auditing
- TACACS+
  - The latest Cisco proprietary version of TACACS
  - Not backwards compatible
  - More authentication requests and response codes

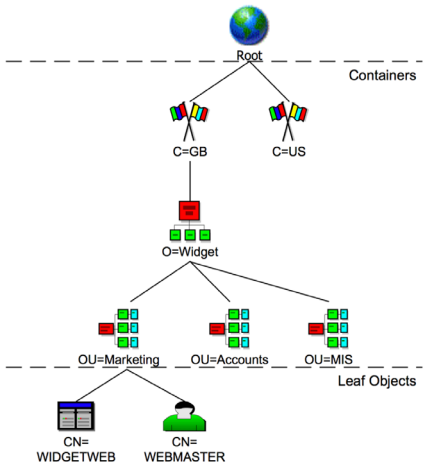


LDAP and Secure LDAP

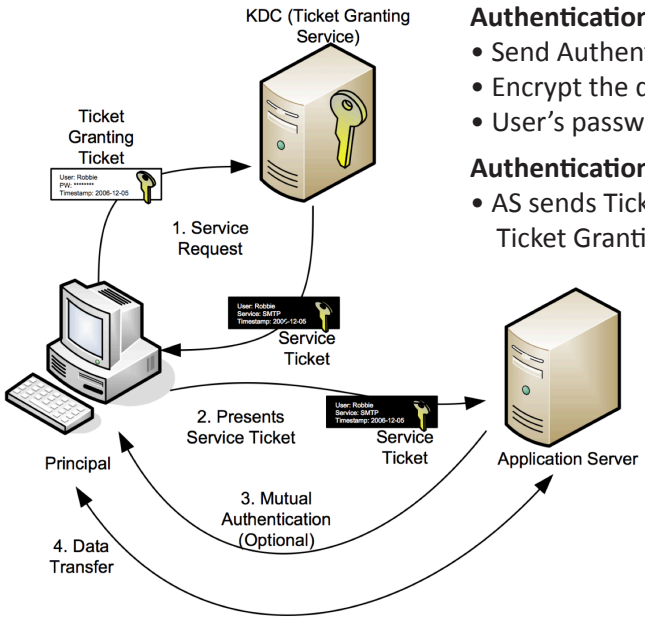
LDAP (Lightweight Directory Access Protocol)
- Protocol for reading and writing directories over an IP network
- X.500 specification was written by the International Telecommunications Union (ITU)
- LDAP is lightweight, and uses TCP/IP (tcp/389 and udp/389)
- LDAP is the protocol used to query and update an X.500 directory
- Used in Windows Active Directory, Apple OpenDirectory, Novell eDirectory, etc.

X.500 Directory Information Tree
- LDAP User Access and Security
- Simple Authentication and Security Layer (SASL) in LDAP v3
- Usually two levels of access - Read-only (query) and read-write (update)

Secure LDAP
- LDAP over SSL - Encrypt with SSL/TLS
- Commonly configured in Microsoft environments - Active Directory uses TCP port 636



Kerberos



Authentication Step 1:
- Send Authentication Service (AS) a logon request
- Encrypt the data and time on the local computer
- User's password hash is the key

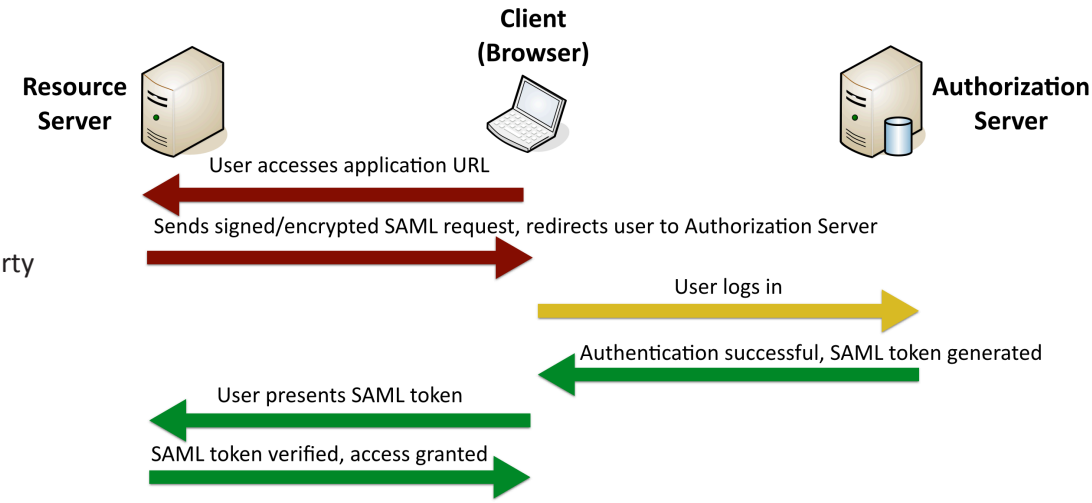
Authentication Step 2:
- AS sends Ticket Granting Ticket (TGT) and Ticket Granting Service (TGS) Session Key

Client Service Authentication Step 1:
- Sends TGS a copy of the TGT and the name the application server
- Time stamped client ID, encrypted with TGS key

Client Service Authentication Step 2:
- Sends the application server the encrypted service ticket and another time-stamped authenticator

Client Service Authentication Step 3:
- App server decrypts the service ticket to confirm an untampered message
- App server decrypts authenticator with service session key
- App server may respond with a timestamp to allow client to verify no man-in-the-middle.

SAML



SAML
- You need access to resources on a service provider
  - You can authenticate through a third-party
- Service provider
  - You need access to this web server
- Client
  - The user that needs access, often from a browser
- Identity Provider
  - The owner of the identities and credentials

Identification, Authentication, and Access Control

Identification vs. authentication
- Identification associates a user with an action
- Authentication proves a user is who it claims to be
- The access control process
  - Prove a user is who they say they are (authorization)
  - Prove a user performed an action (non-repudiation)

Authentication
- Proves a user or process is who it claims to be
- Provide a username and a secret passphrase
- Many different authentication types

Authorization
- Now you're identified - What rights and permissions do you have?
- Policy definition - What rights and permissions should apply?
- Policy enforcement - Only authorized rights are exercised
  - Allow and deny based on defined policies

Access Control
- Authorization
  - Ensure only authorized rights are exercised (policy enforcement)
- The process of determining rights (policy definition)

Access Control Models
- Discretionary access control (DAC)
  - The owner is in full control
  - Very flexible but very weak security
- Role-based access control (RBAC)
  - Access is based on the role of the user
  - Rights are gained implicitly instead of explicitly
  - Windows Groups can provide role-based access control
- Mandatory Access Control (MAC)
  - Based on security clearance levels
  - Every object gets a label
  - Labeling of objects uses predefined rules

Other Access Control Options
- Rule-based access control
  - A generic term for following the rules
  - Access is determined through system-enforced rules
- Implicit Deny
  - Unless otherwise stated, there's no access of any kind
- Time of Day Restrictions
  - Access control changes depending on the time of day

Identification, Authentication, and Access Control (continued)

Authentication Factors
- Something you know - Password, PIN
- Something you have - Smart card, token
- Something you are - Fingerprint, iris scan

Multi-factor Authentication
- More than one factor
- Something you are - Biometrics
- Something you have - Smart card, USB token, phone text
- Something you know - Password, PIN, screen pattern
- Somewhere you are - GPS information, IP address
- Something you do - Handwriting analysis, typing technique

One-Time Password Algorithms
- HOTP - HMAC-based One-Time Password
  - The keys are based on a secret key and a counter
  - Token-based authentication
    - The hash is different every time
  - Hardware and software tokens available
    - You'll need additional technology to make this work
- TOTP - Time-based One-Time Password
  - Use a secret key and the time of day
  - Secret key is configured ahead of time
    - Timestamps are synchronized via NTP
  - Timestamp usually increments every 30 seconds
    - Put in your username, password, and TOTP code
  - One of the more common OTP methods
    - Used by Google, Facebook, Microsoft, etc.

PAP (Password Authentication Protocol)
- PAP is clear-text authentication
- Unsophisticated, insecure

CHAP (Challenge-Handshake Authentication Protocol)
- Encrypted challenge sent over the network
- Three-way handshake
  - After link is established, server sends a challenge message
  - Client responds with a password hash
  - Server compares received hash with stored hash

Single Sign-on (SSO)
- Authenticate one time
- Kerberos authentication and authorization
- 3rd-party options

SSO with Kerberos
- Authenticate one time
- No constant username and password input
- Not everything is Kerberos-friendly

SSO for everything
- Software as a Service (SaaS)
- Many 3rd-party services are available

Federation
- Provide network access to others - Not just employees
- Third-parties can establish a federated network
- Authenticate and authorize between the two organizations
  - Login with your Facebook credentials
- The third-parties much establish a trust relationship
  - And the degree of the trust

Transitive Trust
- One-way trust
  - Domain B trusts Domain A, Domain A doesn't trust Domain B
- Two-way trust
  - Both domains are peers, both trust each other equally
- Non-transitive trust
  - A trust is specifically created and applies only to that trust
- Transitive trust
  - Domain A trusts Domain B, Domain B trusts Domain C, therefore Domain A trusts Domain C

Account Security Best Practices

Role-based Management
- Define groups based on a user's role
- Make the definitions tight enough to apply security controls
- There may be different permissions in the same department
- A user can logically only have rights for one role at a time

Shared Accounts
- Authentication details for one account is known by more than one person
- Sharing accounts makes auditing very difficult,
  - Breaks non-repudiation
  - Activities on a shared account can be challenged
- The account credentials are more likely to be compromised
- Changing the password will involve many people

Protecting Credentials
- All that stands between the outside world and all of the data
- Passwords must not be embedded in the application
- Everything needs to reside on the server, not the client
- Communication across the network should be encrypted
- Authentication traffic should be impossible to see

Group Policy
- Apply security and admin settings across many computers
- Different than NTFS or Share permissions
  - Control the use of the operating system
- Linked to Active Directory administrative boundaries
  - Sites, domains, organization units (OUs)
  - Define by groups, locations, etc.

Group Policy Control
- Administrative policies
  - Remove Add or Remove Programs
  - Prohibit changing sounds
  - Allow font downloads
  - Only allow approved domains to use
  - ActiveX controls without prompt
- Security policies
  - Specify minimum password length
  - Require smart card
  - Maximum security log size
  - Enforce user login restrictions

Account Security Best Practices (continued)

Password Complexity and Length
- Make your password strong
- No single words, no obvious passwords
- Mix upper and lower case, use special characters
- A strong password is at least 8 characters
- Prevent password reuse

Password Expiration and Recovery
- All passwords should expire, change every 30 days, 60 days, etc.
- Critical systems might change more frequently
- The recovery process should not be trivial!
- Some organizations have a very formal process

Account lockout and disablement
- Too many bad passwords will cause a lockout
- This can cause big issues for service accounts
- Disabling accounts is usually part of the normal change process
- You don't want to delete accounts, at least not initially

User Management
- Individual users are granted specific rights
- Difficult to make global changes
- Doesn't scale very well

Group Management
- Put users into a single group, then set privileges on the group
- Add/remove users from the group to assign privileges
- Users can be members of multiple groups
- Group permissions can overlap

Role-based Management
- Based on the role of the user
- Administrators, Users, HR managers, Accounting analysts
- Users can be moved in and out of a role as their job changes
- A user should only have rights for one role at a time

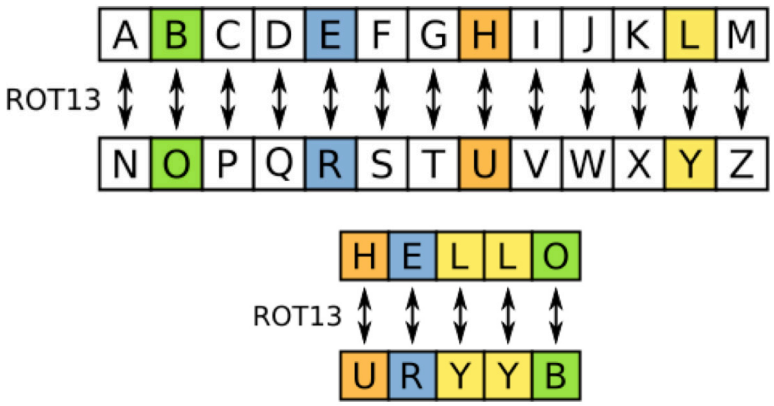
User Access Review
- There can be misconfigurations, changes in user policies
- Auditing should occur often
- Monitor group membership
- Review access control lists
- Identify and disable unused accounts
- Disable unnecessary accounts

Monitoring Event Logs
- Keep a list of every action, i.e., application, security, audit
- This can be an enormous database
- Don't turn these off!
- Use to detect unauthorized access to a resource

General Cryptography Concepts

- Plaintext - An unencrypted message (in the clear)
- Ciphertext - An encrypted message
- Cipher - The algoithm used to encrypt and/or decrypt
- Cryptanalysis - The art of cracking encryption

Substitution Cipher (Caesar cipher)
- Substitute one letter with another - ROT13
  - "Uryyb Jbeyq" is "Hello World"
- Transposition Cipher
  - Keep the letters, change the order - "HLOOLELWRD"
- Hack these ciphers with a frequency analysis



Other Ciphers
- Mechanical Cipher - Germany's Enigma machine (WW II)
- Mathematical Ciphers - Use complex algorithms to encrypt
- Keys - Add the key to the cypher to really encrypt
- One-time pad
  - The plaintext was combined with a shared "pad" of text to produce the ciphertext
  - The decryption would be done with the same pad of text

Symmetric Encryption
- A single, shared key
  - Encrypt with the key, decrypt with the same key
- If the key is found, all data can be decrypted
- Very fast to use, not a lot of overhead
- Often combined with asymmetric encryption

Asymmetric encryption
- Public key cryptography
- Private key - keep this private
- Public key - give to everyone
- The private key is the only key that can decrypt data encrypted with the public key
- You can't derive the private key from the public key

Key Exchange
- Out-of-band key exchange
  - Don't send the symmetric key over the 'net
  - Telephone, courier, in-person, etc.
- In-band key exchange
  - It's on the network
  - Protect the key with additional encryption
  - Often uses asymmetric encryption to deliver a symmetric key

Real-time Encryption/Decryption
- There's a need for fast security
  - Without compromising the security part
- Share a symmetric session key using asymmetric encryption
  - Client encrypts a random (symmetric) key with a server's public key
  - The server decrypts this shared key and uses it to encrypt data
  - This is the session key
- Implement session keys carefully
  - Need to be changed often (ephemeral keys)
  - Need to be unpredictable

General Cryptography Concepts (continued)

Block Ciphers
- Used in symmetric encryption
  - Not used in asymmetric encryption
- Encrypt fixed-length groups (blocks)
  - Often 64-bit or 128-bit blocks
  - Pad added to short blocks to fill the block size
- Confusion
  - The key-to-ciphertext relationship should be very complicated
  - You can't determine the key based on the ciphertext
- Diffusion
  - Output should depend on the input in a complex way
  - If you change one bit of the input, at least 50% of the output should be different

Stream Ciphers
- Also used with symmetric encryption
- Encryption is done one bit or byte at a time
  - High speed, low hardware complexity
- The starting state should never be the same twice
  - Key is often combined with an initialization vector (IV)

Non-repudiation
- Proof of integrity
- Proof of origin, with high assurance of authenticity
- Used for digital signatures
  - Digitally "sign" your files/messages with your private key
  - Others check with your public key

Hashes
- Represent data as a short string of text (a message digest)
- Impossible to recover the original message from the digest
- Used to store passwords and provide confidentiality
- Can be a digital signature for authentication, non-repudiation, and integrity
- A well designed hash will not collide
  - Different messages will not have the same hash

Key Escrow
- A trusted third-party holds the keys
- Allows for recovery of encrypted data

Key escrow with encryption types
- Symmetric encryption - Hide a key in a safe
- Asymmetric encryption - Add an additional private decryption key
- The process is just as important as the key
  - When do you get the key? Who has access? Is there more than one key?

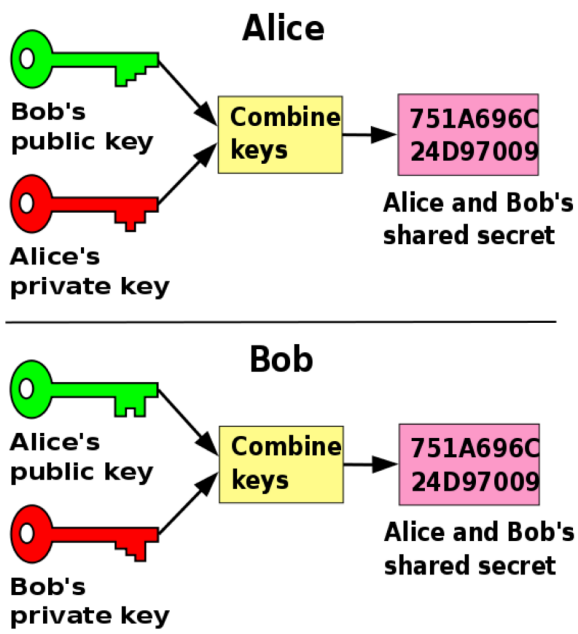
Steganography
- Greek for "concealed writing"
- Message is invisible, but it's really there
- The covertext is the container document or file
- Network based steganography
  - Embed messages in TCP packets
- Embed a message in an image
- Use (nearly) invisible watermarks
  - Yellow dots on printers

Elliptic curve cryptography (ECC)
- Asymmetric encryption
  - Need large integers composed of two or more large prime factors
- Instead of numbers, use curves!
  - Smaller storage and transmission requirements
  - Perfect for mobile devices

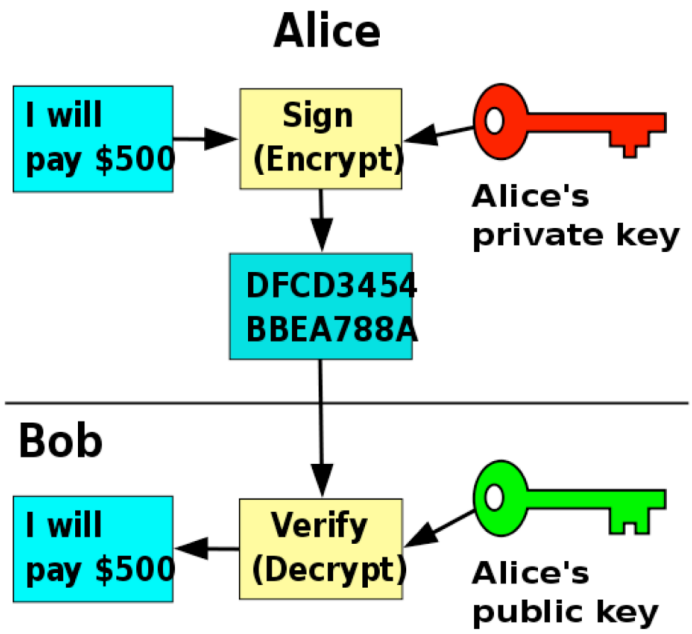
Quantum cryptography
- Use quantum physics to provide cryptographic references
- Quantum key distribution (QKD)
- Used to communicate a shared key between two users
- If a third-party tries to get in the middle, the data is disturbed

Perfect Forward Secrecy (PFS)
- Don't use the server's RSA key pair
- Use Elliptic curve, Diffie-Hellman ephemeral
  - The keys aren't kept around
- You can't recover the key, so you can't decrypt
- PFS requires more computing power - Not all servers use PFS
- The browser must support PFS
  - Check your SSL/TLS information for details

Diffie-Hellman Key Exchange



Digital Signatures



Cryptographic Hash Functions

MD5 Message Digest Algorithm
- First published: April 1992
- Replaced MD4
- 128-bit hash value
- 1996: Vulnerabilities found - not collision resistant
- December 2008: Researchers created CA certificate that appeared legitimate when MD5 is checked

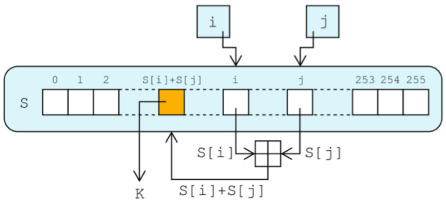
Secure Hash Algorithm (SHA)
- Developed by the National Security Agency (NSA)
- A US Federal Information Processing Standard
- SHA-1
  - Widely used
  - 160-bit digest
  - 2005: Collision attacks published
- SHA-2
  - The preferred SHA variant
  - Up to 512-bit digests
  - SHA-1 is now retired for most US Government use

RIPEMD
- A family of message digest algorithms
- RACE Integrity Primitives Evaluation Message Digest
- RACE - Research and Development in Advanced Communications Technologies in Europe
- Original RIPEMD was found to have collision issues (2004)
- Effectively replaced with RIPEMD-160 (no known collision issues)
- Based upon MD4 design but performs similar to SHA-1
- RPIEMD-128, RIPEMD-256, RIPEMD-320

HMAC
- Hash-based Message Authentication Code
  - Combine a hash with a secret key
  - e.g., HMAC-MD5, HMAC-SH1
- • Verify data integrity and authenticity
  - No fancy asymmetric encryption required
- • Used in network encryption protocols
  - IPsec, TLS

Symmetric Encryption Ciphers

RC4
- Rivest Cipher 4 - Ron Rivest (Ron's Code 4)
- RC4 has "biased output"
  - If the third byte of the original state is zero and the second byte is not equal to two, then the second output byte is always zero
- Not common to see RC4 these days



DES and 3DES
- Data Encryption Standard - DES and Triple DES
- One of the Federal Information Processing Standards (FIPS)
- 64-bit block cipher
  - 56-bit key (very small in modern terms)
- 3DES - Use the DES algorithm three times
  - Three keys, two keys, or the same key three times
- Superseded by AES (Advanced Encryption Standard)

AES (Advanced Encryption Standard)
- US Federal Government Standard
- 128-bit block cipher - 128-, 192-, and 256-bit keys
- Used in WPA2 - Powerful wireless encryption

Blowfish
- Designed in 1993 by Bruce Schneier
- 64-bit block cipher, variable length key (1 to 448 bits)
- No known way to break the full 16 rounds of encryption
- One of the first secure ciphers not limited by patents

Twofish
- Successor to Blowfish
- 128-bit block size, key sizes up to 256
- No patent, public domain

Symmetric Encryption Ciphers

RSA
- Ron Rivest, Adi Shamir, and Leonard Adelman (1977)
- Public-key cryptography system
- Based on the product of two large prime numbers
  - You must know the factors to decode
- Now released into the public domain
  - Used extensively for web site encryption and DRM

Diffie-Hellman Key Exchange
- A key exchange method over an insecure communications channel, published in 1976
- Witfield Diffie and Martin Hellman (and Ralph Merkle)
- DH does not itself encrypt or authenticate
- It's an anonymous key-agreement protocol
- Used for Perfect Forward Secrecy
  - Ephemeral Diffie-Hellman (EDH or DHE)
  - Combine with elliptic curve cryptography for ECDHE

One-Time Pad
- 1917 - Built to encrypt teletype communication
  - Mixed a paper tape (message) with another paper tape (key)
- The "pad" is a pad of paper
  - Very simple encryption and decryption process
- Very secure encryption - Unbreakable when used correctly

One-Time Pad Rules
- The key is the same size as the plaintext
  - The number of letters should be exactly the same
- The key is truly random - no pseudo-random computer functions
- The key should only be used once - destroy after use
- There are only two copies of the key
  - One for the sender, one for the receiver

NTLM

LAN Manager (LANMAN)
- Microsoft and 3Com network operating system
- Hash challenge, similar to CHAP
- Somewhat insecure
  - All uppercase ASCII, password is 14-characters max
  - Passwords over 7 characters are split and encrypted separately
  - Passwords are not salted

NTLM vulnerabilities
- Some Windows password databases contain LM hash versions of the passwords
- NTLM is vulnerable to a credentials forwarding attack

NTLM (NT LAN Manager)
- Used in early versions of Windows NT
  - Password is Unicode and up to 127 characters long
  - Stored as a 128-bit MD4 hash
- NTLMv2 was first seen on Windows NT SP4
  - New password response
  - MD4 password hash (same as NTLMv1)
  - HMAC-MD5 hash of username and server name
  - Variable-length challenge of timestamp, random data, domain name

Transport Encryption Algorithms

SSL (Secure Sockets Layer)
- Developed by Netscape in 1996
- TLS (Transport Layer Security) - Derived from SSL
- HTTPS uses SSL/TLS to encrypt web server communication

SSH (Secure Shell)
- Encrypted console communication
- Used often for remote administration
- Includes secure file transfer (SFTP) and secure file copy (SCP)

IPsec
- Security for OSI Layer 3
- Encrypts IP packets (tcp/udp 1293)
- Provides confidentiality and integrity/anti-replay
- Encryption and packet signing
- Very standardized
- Two core IPsec protocols are Authentication Header (AH) and Encapsulation Security Payload (ESP)

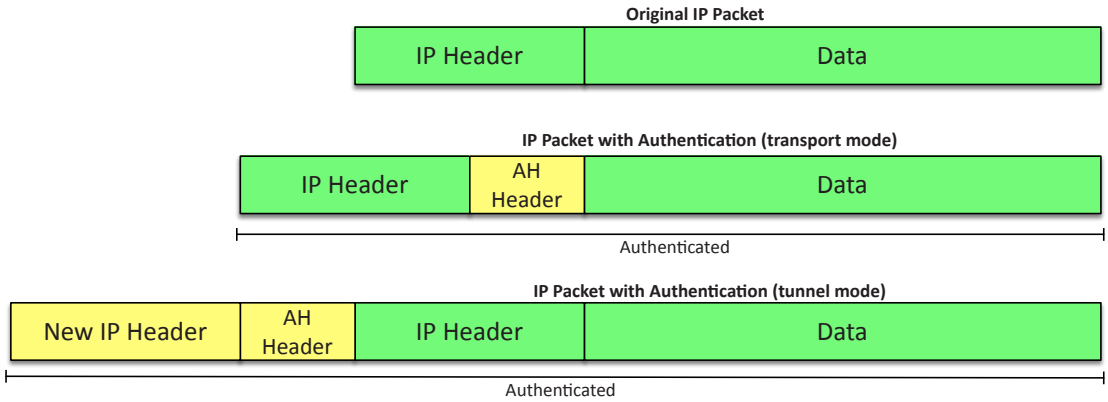
IPsec Authentication Header (AH)

Transport mode
- Only IP payload is encrypted and/or authenticated

Tunnel mode
- Entire packet is encrypted and/or authenticated

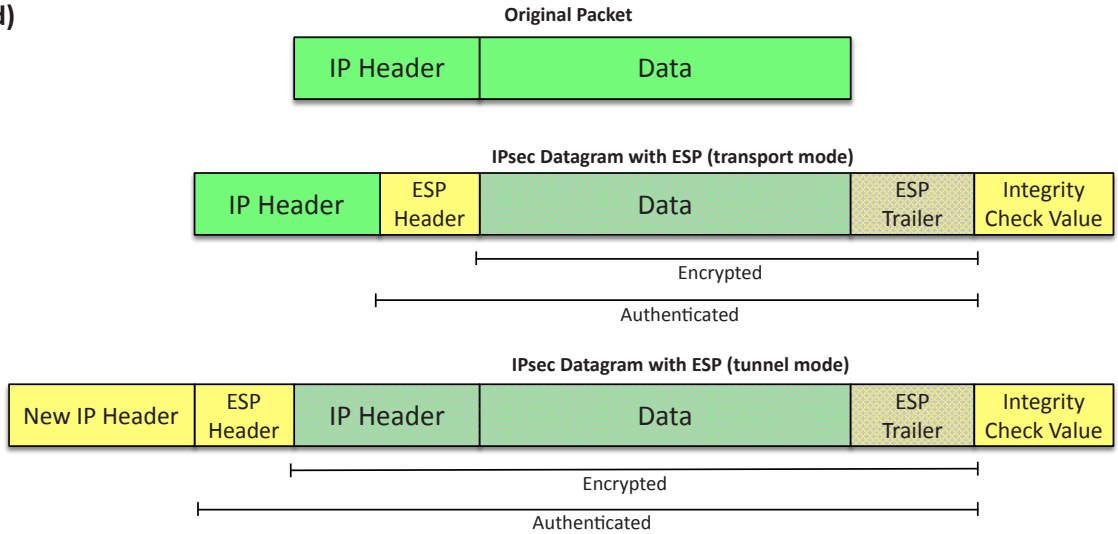
AH (Authentication Header)
- Data integrity
- Origin authentication
- Replay attack protection
- Keyed-hash mechanism
- No confidentiality (encryption)

Building the Authentication Header
- Hash of the packet and a shared key
- Often uses a well-known hash
  - MD5, SHA-1, or SHA-2
- The AH is added to the packet header



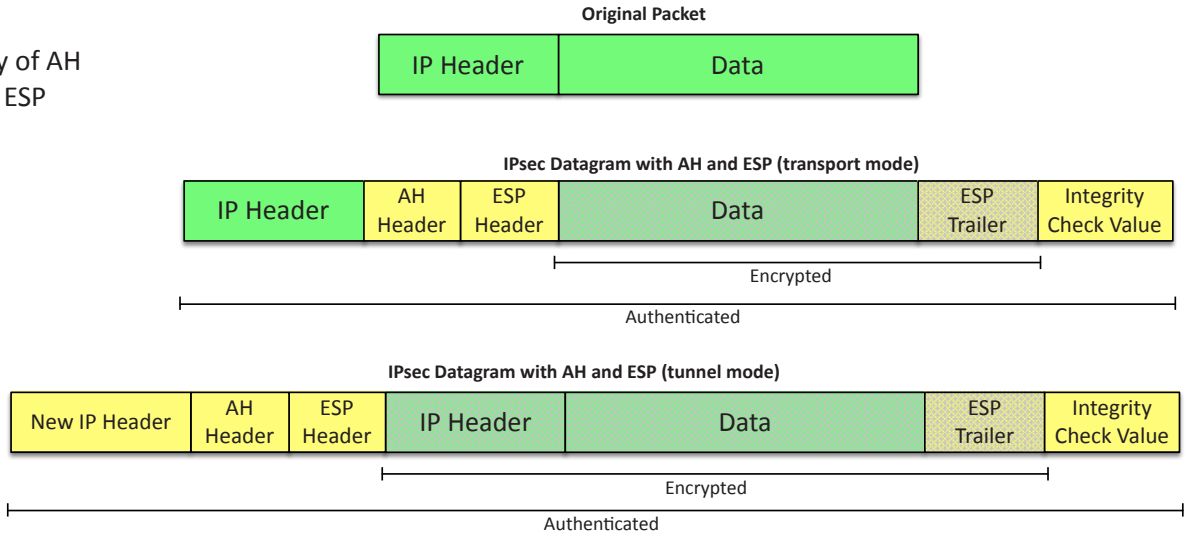
IPsec Encapsulating Security Payload (ESP)

ESP (Encapsulating Security Payload)
- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity
- Anti-replay protection



IPsec with AH and ESP

AH and ESP
- Combine the data integrity of AH with the confidentiality of ESP



Strong vs. Weak Encryption

The Strength of Encryption
- Practically everything can be brute forced
- Strong algorithms have been around for a while
  - That's part of the reason that they are strong
  - Wired Equivalent Privacy (WEP) was found to have design flaws
- Strong algorithms - PGP, AES
- Weak algorithms - DES (56-bit keys), WEP (design flaw)

Key Stretching
- A weak key is a weak key - by itself, it's not very secure
- Make a weak key stronger by performing multiple processes
  - Hash a password. Hash the hash of the password. And continue…
- Brute force attacks would require reversing each of those hashes
  - The attacker has to spend much more time, even though the key is small

Key stretching libraries
- bcrypt
  - Generates hashes from passwords
  - An extension to the UNIX crypt library
  - Uses Blowfish cipher to perform multiple rounds of hashing
- Password-Based Key Derivation Function 2 (PBKDF2)
  - Part of RSA public key cryptography standards (PKCS #5, RFC 2898)

PKI and Certificate Management

Commercial certificate authorities
- Built-in to your browser
- Purchase your web site certificate
  - It will be trusted by everyone's browser
- Create a key pair, send the public key to the CA to be signed
  - A certificate signing request (CSR)
- May provide different levels of trust and additional features
  - Add a new "tag" to your web site

Private certificate authorities
- You are your own CA - build it in-house
- Needed for medium-to-large organizations
- Implement as part of your overall computing strategy
  - Windows Certificate Services
  - OpenCA

Key Revocation
- Certificate Revocation List (CRL)
- Maintained by the Certificate Authority (CA)

Getting Revocation Details to the Browser
- OSCP (Online Certificate Status Protocol)
- The browser can check certificate revocation
- Messages usually sent to an OSCP responder via HTTP
- Not all browsers support OSCP
- Early Internet Explorer versions did not support OSCP

Web-of-Trust Key Revocation
- You manage your own certificates
- You must find others to sign your certificate, and those people must be trusted by others
- Plan to revoke your key with a revocation certificate
- You can also enable others to create revocation certs for your key

Public Key Infrastructure (PKI)
- Policies, procedures, hardware, software, people to manage digital certificates
- Create, distribute, manage, store, revoke
- Requires extensive planning
- Also refers to the binding of public keys to people

The Key Management Lifecycle
- Key generation - Create a key with the requested strength using the proper cipher
- Certificate generation - Allocate a key to a user
- Distribution - Makes the key available to the user
- Storage - Secure storage and protection against unauthorized use
- Revocation - Manage keys that have been compromised
- Expiration - A certificate may only have a certain "shelf life"

PKI and Certificate Management (continued)

Key Recovery
- Your private key is valuable
- Backup and store private keys
- Use "M of N" control to restrict access
- Built-in to Windows Server CA and other 3rd-party CAs

Public Keys and Private Keys
- The Key Pair
  - Asymmetric encryption, Public Key Cryptography
- Both the public and private key are built at the same time
- Lots of randomization and large prime numbers

Digital Signatures
- Sign with the private key
  - The message doesn't need to be encrypted
- Verify with the public key
- Any change in the message will invalidate the signature

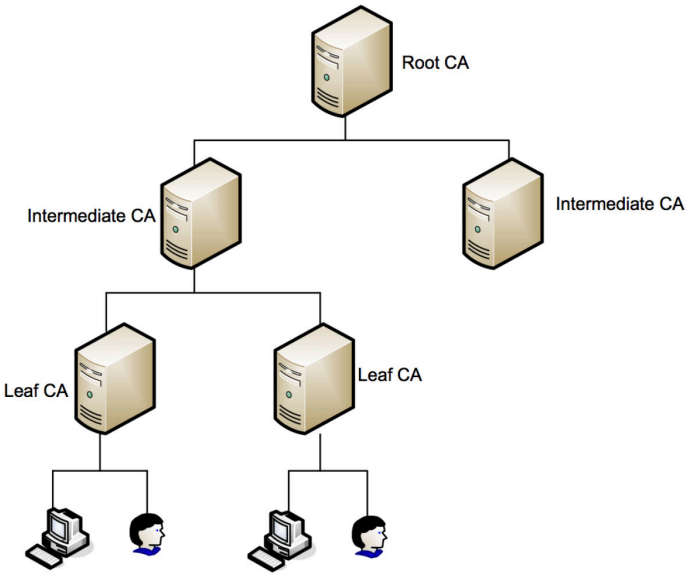
Symmetric key from asymmetric keys
- Use public and private key cryptography to create a symmetric key

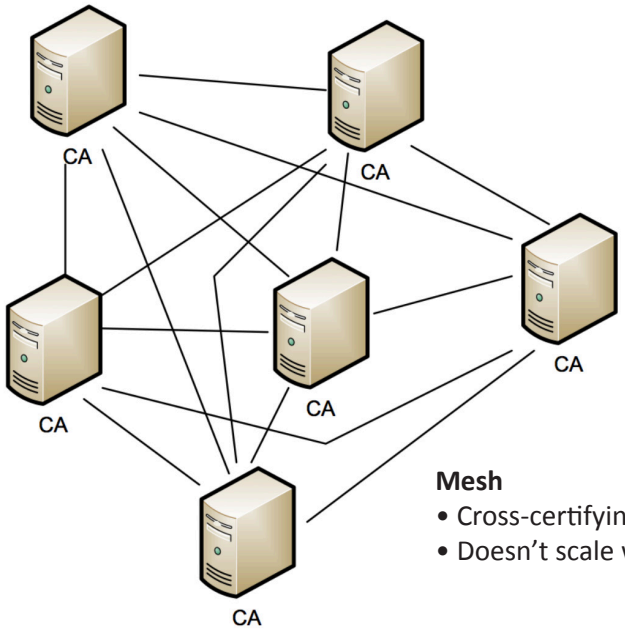
Key Registration
- The Registration Authority (RA) provides the PKI role that ensures the public key is bound to the individual
- Important for non-repudiation
- This can range from a casual verification to a formal, multi-step verification
- Federal Public Key Infrastructure Policy Authority X.509 Certificate Policy for the U.S. Federal Government

Key Escrow
- Someone else holds your decryption keys
  - Your private keys are in the hands of a 3rd-party
- This can be a legitimate business arrangement
  - A business might need access to employee information
  - Government agencies may need to decrypt partner data

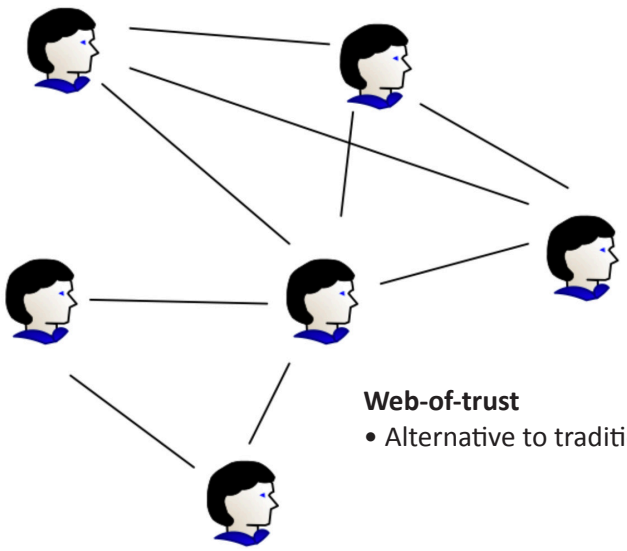
Public Key Infrastructure Trust Models

Single CA
- Everyone receives their certificates from one authority
- Hierarchical
- Single CA issues certs to intermediate CAs





Mesh
- Cross-certifying CAs
- Doesn't scale well



Web-of-trust
- Alternative to traditional PKI

Mutual Authentication
- Server authenticates to the client and the client authenticates to the server