About the Exam

Six major topic areas make up the CompTIA SY0-401 Security+ exam. The topics are as follows:

- Network Security
- Compliance and Operational Security
- Threats and Vulnerabilities
- Application, Data, and Host Security
- Access Control and Identity Management
- Cryptography

This guide will walk you through all the skills measured by the exam, as published by CompTIA

Objectives

Network Security

1.1 Network Devices

1.2 Secure Network Administration

1.3 Secure Network Design Elements

1.4 Network Protocols, Ports, OSI Model

1.5 Secure Wireless

Compliance and Operational Security

2.1 Risk Concepts

2.2 Integrating Systems

2.3 Risk Mitigation

2.4 Forensics

2.5 Incident Response

2.6 Security Training

2.7 Physical Security and Environmental Controls

2.8 Risk Management

2.8 Confidentiality, Integrity, Availability (CIA) and Safety

Threats and Vulnerabilities

3.1 Malware Types

3.2 Attack Types

3.3 Social Engineering Attacks

3.4 Wireless attacks

3.5 Application Attacks

3.6 Attack Mitigation and Deterrence

3.7 Attack Assessment Tools

3.8 Penetration Testing vs. Vulnerability Assessment

Application, Data and Host Security

4.1 Application Security

4.2 Mobile Security

4.3 Host Security

4.3 Data Security

Access Control and Identity Management

5.1 Functions of Authentication Services

5.2 Authentication, Authorization, and Access Control

5.3 Account Management

Cryptography

6.1 Cryptography Concepts

6.2 Cryptographic Methods

6.3 Public Key Infrastructure (PKI)

Network Security

1.1 Network Security

Router Functions

Routers connect networks generally based on network addresses, usually IP network addresses. They create subnets which isolate broadcast domains, and to some extent isolate security zones, particularly when access control lists (ACLs) are implemented. Routers can have a manually /statically configured routing table or use routing protocols to dynamically determine the best path.

Router Security

Routers should be physical secured in a server room. Default passwords should be changed.
Access should be limited to the console port or SSH. TACACS+ is the best method of remote user authentication to a router. ACLs to control allowed traffic should be implemented. ACLs should disallow incoming spoofed addresses, source routing, and broadcasts

Switch Functions

Switches connect hosts on a LAN by MAC address. They reduce or eliminate collisions. VLANs can and should be created on switches. Each VLAN is a broadcast domain and to some extent a security zone. For instance a sniffer on one VLAN cannot see traffic on another VLAN. VLANs are connected by routers or multilayer switches

Switch Security

Client access should be controlled by approved MAC address. This is port security. Unused ports should be disabled. VLANs should be created to isolate broadcast /security domains. Disable Dynamic Trunking Protocol so that an attacker with a sniffer cannot listen to traffic from all VLANs. Change default passwords so an attacker cannot take over a router. To limit attacks, limit remote access and physical access.

VPN Concentrator

Virtual Private Networks (VPNs) encrypt traffic passing through the Internet. It follows that VPNs allow secure remote access. A VPN concentrator allows scalable secure remote access by being able to handle the load of multiple heavily utilized VPN connections.

Load Balancer

A load balancer distributes the load among multiple Web servers, increasing performance, and reliability, while eliminating a single point of failure by providing redundancy

Devices that Inspect Network Packets

Examples of devices that inspect network packets include sniffers, protocol analyzers, NIDS, and NIPS.

Sniffers/Protocol Analyzers

Sniffers capture network packets. They are usually integrated with a protocol analyzers that understand the content of the packets. Examples are Wireshark and Microsoft Network Monitor.

Honeypot and Honeynet

A honeypot is single fake system meant to divert attackers away from a production network and to study hacker tools and techniques. A honeynet emulates a set of servers

NIDs and NIPs

Network based Intrusion detection systems inspect network traffic and do logging and alerting. Network based Intrusion prevention systems take the next step in that they also neutralize attacks.

Types of NIDs & NIPs

Signature based NIDS/NIPS (also HIDS/HIPS) need updates. They are best for known attacks. Anomaly based NIDS/NIPS (also HIDS/HIPS) look for unusual events. They are best for zero day attacks. Behavior based NIDS/NIPS (also HIDS/HIPS) match specifically configured traffic patterns.
Heuristic NIDS/NIPS (also HIDS/HIPS) are similar to anomaly based. They use artificial intelligence to detect new attacks

Filtering Connectivity

To kill connections with an attacker, NIPS do shunning, blocking on attackers, and TCP resets on victims. Firewalls control traffic based on such parameters as ACL, stateful connection inspection, or inspection of the contents of packets at the application layer. A web security gateway / content filter blocks Web sites by URL. A proxy Server caches Web pages, while a reverse Proxy can have sophisticated filters. A SPAM filter is typically incorporated in Email. Finally, an all-in-one security appliance integrates many of the above functions

1.2 Secure Network Administration

Secure Network Administration Elements

Elements of secure network administration include rule-based management, firewall rules, VLAN management, secure router configuration, access control lists, port security, 802.1x, flood guards, loop protection, implicit deny, preventing network bridging by network separation, and log analysis

Secure Network Administration

Secure network administration includes the setup of firewall and router filtering and access control lists including anti-spoofing rules, aided by an understanding of implicit deny. Implicit deny means that any connection not explicitly allowed is denied by default. Passwords for firewalls, routers, and switches should be changed. Administrators should create VLANs, secure ports by MAC address, disable DTP. Switch trunk ports should be mirrored for NIDS/NIPS so all traffic can be monitored / protected. Remote router authentication should be through SSL or 802.1x. Logs for all network devices should be reviewed. Flood guards should be used to protect against SYN flood attacks, trace the source, generate alerts, and block attack traffic. Loop protection prevents network disruption if both ends of a network cable are connected to

different switch ports. Bridging a USB cellular connection to get around a firewall should be disallowed as it may join two networks of different classifications.

1.3 Secure Network Design Elements

Secure Network Design Elements

The following are components of a secure network design: DMZ, subnets, VLANs, NAT, secure Remote Access, hardening of telephony, NAC, virtualization, judicious use of cloud computing including Platform as a Service, Software as a Service, and Infrastructure as a Service. Additional elements are a De-Militarized Zone (DMZ) which is an area between two firewalls. The first firewall protects Web and other public facing servers from threats on the Internet. The second firewall more completely protects the internal network.

Subnetting and VLANs

Subnets and VLANs separate broadcast and to some extent security domains. Subnets are created on routers. VLANs are created on switches. On switches, DTP should be disabled to prevent VLAN jumping, and port spanning/port mirroring should be disabled on trunk ports except for NIDS/NIPS use.

Network Address Translation

NAT conserves and hides IP addresses. Static NAT has a one to one mapping between internal and external addresses. Dynamic NAT allows that mapping to change dynamically. Port Address Translation (PAT) allows multiple hosts to connect at the same time. NAT Transversal (NAT-T) works with IPSEC that also rewrites the IP header .

Remote Access

Remote access policy sets rules for remote access. Remote access should use a secure protocol such as SSH. Finally a VPN concentrator would provide remote access for a large number of users

Telephony

Telephone switches should be physically secured. Default passwords should be changed. If remote administration is allowed it should be via a secure protocol such as SSH, not Telnet, or SNMP.

Network Access Control (NAC)

NAC would redirect a guest user to the company portal and ask the user to agree to the company's acceptable use policy. NAC checks out and remediates foreign laptops that attempt to connect to a company network. It also updates patches and antivirus definitions and performs a virus scan before granting access to a corporate network. Finally, NAC provides levels of network access based on predetermined characteristics.

Virtualization

In virtualization, one or more physical servers host multiple virtual servers. This cuts down on the footprint. If you have only one physical server then this is a single point of failure, but if you have multiple physical servers operating as a virtualization farm then availability increases. The specialized operating system that hosts the virtual machines is the hypervisor. The host and guest OSs should all be patched, as virtual machines have the same security requirements are physical servers. In general virtual machines are isolated

and are a safe environment to test malware. To prevent reverse engineering, some malware can detect a virtual environment. Memory can be shared between the host virtual machines and could be attacked to harm all of them. Finally escape is the term for an attack that affects more than one virtual machine.

Cloud Computing

Cloud computing utilizes hosted services over the Internet. It is sold on demand and is elastic, using virtualization to provision guests on demand. It is also fully managed by the provider, facilitating computing for heavily utilized systems. Security drawbacks of cloud computing are loss of physical control over data, and blended systems and data.

Cloud Computing Services

In Platform as a Service (PaaS) developers create applications on the provider's platform. PaaS is an easy-to-configure OS with on-demand computing. In Software as a Service (SaaS) the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. A company would not have to hire additional personnel or servers and could minimize the footprint of their datacenter. In Infrastructure as a Service (IaaS) users can start, stop and configure virtual servers. It would be useful to a company with a lot of sensitive data on unreliable systems

1.4 Secure and Insecure Network Protocols

Secure and Insecure Network Protocols

Network protocols include IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SFTP, SCP, ICMP, as well as IPv4 and IPv6.

IPSEC

IPSEC was originally developed for IPv6. IPSEC protocols include ESP, AH, and IKE. ESP provides confidentiality through encryption. AH provides message integrity, non-repudiation, authentication, and protection from replay attacks through a hash. ESP is stronger than AH. ESP plus AH is strongest
IKE manages security keys and associations. IPSEC can be used as the encryption piece of a VPN with L2TP setting up the tunnel, or IPSEC can be the tunneling and encryption piece of a VPN

SNMP

SNMP is used to manage network devices including printers, servers, routers, and switches. SNMPv1 and SNMPv2 are insecure protocols. SNMPv3 is secure and provides data integrity, authentication, confidentiality, and protection from malicious reordering of the data stream. SNMP can be used to consolidate logging information from various servers and network devices.

SSH

SSH is a secure replacement for Telnet and FTP. Slogin replaces Telnet. SCP and SFTP replace FTP. FTPS is another secure version of FTP, but it is not based on SSH

DNS

DNS resolves a host name to an IP address. It replaces, but operates alongside a Hosts file. DNS footprinting enumerates the hosts on a network. While DNS kiting reregisters a domain name within the five day grace period. DNS attacks include spoofing and cache poisoning. To detect DNS attacks,
DNS logs should be evaluated for failed zone transfers and attempted zone transfers to an unknown host. NSLookup should not allow a zone transfer.

HTTP, HTTPS, SSL and TLS

HTTP transfers Web pages. HTTPS does this securely using certificates. SSL is the underlying protocol for HTTPS. SSL can also be used in SSTP to set up a VPN that does not require a VPN client setup. TLS is more secure than SSL because it checks that a certificate belongs to the web site, it also can be used to secure traffic between SMTP servers

TCP/IP

IP provides addressing and routing. An attacker can forge the source IP address. TCP provides reliability through sequence numbers. An attacker might monitor a network transmissions predict a sequence number and forge an acceptable response. This is a Man-in-the-Middle attack. Finally, the three-way TCP handshake can be exploited in a SYN Flood attack

ICMP

ICMP provides network reachability and diagnostics. It supports ping, tracert, and router messages such as source routing. ICMP attacks include Ping of Death, Surf Attack, and bogus source routing updates. Source routing should be disabled. Firewalls should block ping packets and have anti-spoofing rules. Responses to the subnet broadcast address should be disabled

IPv4 vs. IPv6

IPv4 has a 32 bit address space that is depleted. IPv6 has a 128 bit address, enough for 100 IP addresses for every square inch on the earth. It was designed with security in mind with original support for IPSEC, so it provides secure tunneling services

1.5 Network Ports

These port numbers should be memorized:

General

FTP 20/21
FTPS 989/990
SSH, SCP, SFTP, SLogin 22
TELNET 23
NetBIOS 139 /445
Radius 1812/1813

Web

HTTP 80
HTTP Admin 8080
HTTPS 443

Email
SMTP 25
POP3 110
IMAP4 143

Networking
DNS 53
DHCP 67/68
RDP 3389

Active Directory
Kerberos 88
LDAP 389/636

VPNs
L2TP 1701
PPTP 1723
IKE 500
IKE Protocol ID 50

1.6 Secure Wireless

Secure Wireless Elements
Elements of secure wireless include WPA, WPA2, WEP, EAP, PEAP, LEAP, MAC filters, disabling SSID broadcast, TKIP, CCMP, proper antenna placement, and low power levels.

Securing Wireless Routers
Filter by MAC address. Measures to secure wireless routers include changing the SSID and disabling SSID broadcast. As defenses against war driving, change the default password and only allow secure remote administration. Use the lowest power level that does the job, place the antenna in the center of the building, and use shielding and /or directional antennas.

Wireless Router Encryption
WEP is weak. It has a 24 bit initialization vector. It should not be used. WPA is much stronger as it uses EAP, TKIP, and RC4. WPA2 replaces RC4 with AES. 802.11i is better than WPA2 as it replaces TKIP with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP changes the whole encryption key on a minute by minute basis, while TKIP changes only part of the encryption key.

PSK vs. Enterprise
In general WPA2 is stronger than WPA. WPA or WPA2 Personal/PSK use a passphrase/pre-shared key. This is not as secure as WPA or WPA2 Enterprise which uses a longer key or a that is machine generated and unknown to users. Enterprise also uses 802.1X, so WPA Enterprise is stronger than WPA2 Personal.

EAP, EAP-TLS, PEAP, & LEAP
EAP is Extensible Authentication Protocol. WPA/WPA2 Enterprise use EAP. EAP-TLS uses certificates. PEAP is Protected EAP encapsulates EAP in an encrypted and authenticated

TLS tunnel. It also uses certificates and MS-CHAPv2 to perform mutual authentication. LEAP is Lightweight EAP uses MS-CHAPv2 to protect authentication credentials and provide mutual authentication.

Compliance and Operational Security

2.1 Risk Concepts

Risk Concepts

Risk concepts include the types of risk control, procedures to minimize false positives, the importance of policies in reducing risk, the differences between quantitative and qualitative risk assessments, also ways to handle risk such as risk-avoidance, transference, acceptance, mitigation, deterrence, and finally risks associated with cloud computing and virtualization.

Risk Controls

Technical risk controls would use such technical devices such as firewalls, IDSs/ IPSs, ACLs, proximity locks, and mantraps. Management controls would avoid single points of failure, and include fault-tolerant measures, and recovery procedures. Operational risk controls include auditing, user rights review, and background investigations, due care and due diligence to limit risk exposure caused by inadequate internal processes, people and systems.

False Positives/False Negatives

The Crossover Error Rate represents the proportion of false alerts. In intrusion detection systems a false negative is where an attack is not identified is more serious than a false positive. In Biometrics a false acceptance is more serious that a false rejection. The process of tuning eventually reduces the crossover error rate where the number of false positives equals the number of false negatives.

Policies that Reduce Risk

Risk reduction starts at the management level where security policies are set that identify and protect critical assets. For instance, the risk of open ports on a switch can be reduced by a policy to enable MAC filtering, and the risk of a known attack can be reduced by a patch management policy.

Quantitative vs. Qualitative

Quantitative is based on hard numbers while qualitative is based on subjective ranking. Quantitative is based on asset value and exposure, so risks are mitigated based on cost. It is quicker to do a qualitative risk assessment.

Responses to Risk

Risks can be accepted if the cost to mitigate the risk is more than the cost of the asset. Risks can be avoided if the loss of the asset is unacceptable. In some cases, risks can be transferred to an insurance company. Most mission impacting risks should be mitigated. However, risks cannot be eliminated. Finally, risk deterrence is a policy to make attackers think twice based on the likelihood of retaliation.

Cloud Computing and Virtualization Risks

Cloud computing uses virtualization to provision guests on demand. Security drawbacks of cloud computing are loss of physical control over data, and blended systems and data. Moreover, if you have only one physical server hosting multiple virtual servers then this is a single point of failure.

2.2 Risk Mitigation

Risk Mitigation Elements

Implement security controls based on risk. Form a change management committee. Create and exercise plans to respond to incidents. Perform user rights and permissions reviews. Set up auditing procedures. Finally, implement policies and procedures to prevent data loss or theft.

Implement Security Controls Based on Risk

Most mission impacting risks should be mitigated, while Show stopping risks should be avoided. Fault tolerant measures and disaster recovery plans should be based on a cost-benefit analysis. Insurance should be used to transfer high impact risks, while minor, low-probability risks are a cost of doing business and should be accepted if there isn't a low cost countermeasure.

Change Management

Change management is the orderly process for handling system upgrades and modifications so that they do not impact security. For instance, an administrator updating software or hardware should document the work in a change management system. Another example is that critical patches for a server should not be delayed until the next change management meeting, but they should be documented.

Incident Management

In incident management a security administrator performs various audits of a specific system after an attack. It ensures that that the proper configurations are reapplied to systems, are attacks are contained. An example of containment would be to disable a network connection after an attack.

2.3 Incident Response

Incident Response Elements

Components of incident response include basic forensic procedures, damage and loss control, chain of custody, and first responder incident response.

Basic Incident Response

Notify the incident response team. Most important on the team are administrators and data owners

Secure the area. This would include crime scene tape. Contain the incident. Analyze the most perishable material first such as memory, the arp cache, and temporary files. Create an image of the hard drive. Remember to perform a hash before and after the image and hash the imaged hard drive. Finally, compare hashes.

Damage and Loss Control

Consistent with collecting evidence, contain the incident. Analyze the attack to prevent future attacks of a similar nature. The last step in incident response is updating procedures based on lessons learned.

Chain of Custody

Chain of custody is continuously documenting state and location of data and hardware from collection to disposition. An example would be to document who transported a hard drive during an incident response. An example of a violation of the chain of custody would be if an SD memory card collected for a forensic analysis was left unguarded

Incident First Responders

First responders should secure the area and perform proper forensics with documentation along the way, initiating the chain of custody. This might include videotaping with comments on actions taken. The files and utilities on the compromised system should not be trusted. The most perishable information should be collected first. Hard drive forensics should be performed on a bit-by-bit copy of the hard drive.

2.4 Security Training

Security Training Elements

Elements of security training include security policies and procedures, protection of personally identifiable information, proper information classification based on the sensitivity of hardware and software. Additional components include data labeling, handling and disposal requirements, in accordance with laws, best practices and standards. Training should improve user awareness and responses to threats including social engineering, and the vulnerabilities of social networking and P2P software.

Security Policy Training

This puts users on the security team and educates them about threats and countermeasures. It trains them in mandatory security procedures and recommended best practices. It reduces the likelihood of successful social engineering attacks. It is required for compliance with laws, best practices, and standards. Users are warned of the consequences for their organization and themselves for non-compliance. Users should be trained on protecting personally identifiable information and sensitive corporate data. This includes protection from shoulder surfing. It also includes data labeling and protection by

classification. Training should emphasize that software and hardware should be sanitized before disposal. For instance hard drives can be shredded or degaussed. Finally, users should be educated to avoid disclosing information via social networking sites and/or P2P file sharing

2.5 Business Continuity

Business Continuity Elements

The components of business continuity planning include business impact analysis, removing single points of failure, business continuity planning and testing, continuity of operations, disaster recovery, IT contingency planning, and succession planning.

Business Impact Analysis (BIA)

A BIA is a high level analysis that identifies a company's exposure to the sudden loss of critical business functions. It involves assessing both financial and non-financial costs during business disruption and business restoration periods. BIA defines Recovery Point Objectives and Recovery Time Objectives. After a BIA a decision might be made to build a redundant data center.

Removing Single Points of Failure

Measures that remove single points of failure include RAID, clustered servers, redundant power supplies, and redundant ISPs. One database server feed by five Web servers would be a single point of failure. A single database administrator would also be a single point of failure. Two final example of single points of failure are a CRL and a SSO.

Business Continuity Planning (BCP) and Testing

A BIA collects business unit requirements which is the main input to BCPs. Depending on how long a critical application can be unavailable, BCP will dictate a hot, warm, or cold backup site. If full testing is not available BCPs should be exercised with table top exercises. Regularly exercising business continuity plans will discover single points of failure.

Continuity of Operations

A Continuity of Operations Plan (COOP) defines and provides for the nearly uninterrupted operation of mission essential functions. It facilitates decision making in a crisis to ensure near continuous performance and protects essential assets, while reducing damage and losses, and expediting an orderly resumption of full business operations

Disaster Recovery

Disaster recovery's goal is timely resumption of important IT functions to include alternate sites and backups. It would include company restoring a critical system after a disruption or failure. Auditing and logging of transactions should be recovered first. Plans should be tested regularly.

IT Contingency Planning

The IT continuity plan prepares for the resumption of IT functions after a disruption. It identifies show stopping issues that might limit interim business processing. It is a subset of risk management in which costs and benefits of alternate IT backup and recovery plans are evaluated.

Succession Planning

Succession planning applies to contingency plans to replace key personnel in an emergency such as a CIO being involved in a airplane crash. A prime example of this is moving the Vice President of the US to an alternate location in the event of a nuclear attack. It could be applied to critical IT personnel as in the case of Apple's planning for the replacement of Steve Jobs.

2.6 Environmental Controls

Environmental Control Elements

Environmental control elements include HVAC, fire suppression, EMI shielding, hot and cold aisles, environmental monitoring, and video monitoring.

HVAC

HVAC is heating, ventilation and air conditioning. HVAC is used to maintain proper environmental conditions in a datacenter. If proper HVAC is not maintained, systems availability is compromised.

Attackers may be able to remotely destroy critical equipment in the datacenter by gaining control of HVAC.

Fire Suppression

HVAC systems should be should be integrated into the fire alarm systems to help prevent a fire from spreading and should shut down when a fire is detected in the datacenter. Carbon dioxide (CO2) is the best suppression method for a Class C fire so no equipment is damaged when encountering a fire or false alarm. In a fire, electronic cipher locks should allow personnel to exit the building without any forms of authentication.

EMI Shielding

EMI is Electro Magnetic Interference while RMI is Radio Magnetic Interference. If air conditioning affects wireless connectivity, shielding should be used to stop RFI. The following cable types provide EMI protection: fiber optic, coaxial, and STP. EMI could affect backups.

Hot and Cold Aisles

Hot and cold aisles regulate cooling within a datacenter to maximize airflow, increase HVAC efficiency, and save utility costs.

Environmental Monitoring

Environmental monitoring includes video monitoring and humidity controls. It uses temperature and humidity sensors, power meters, as well as airflow and efficiency measurements. Alerts are automatic. HVAC issues are quickly contained and operating costs are lowered.

Temperature & Humidity Controls

Thermostats control temperature. Too high a temperature would lead to server breakdowns. Humidistats control humidity. Too low humidity would increase the likelihood of static discharges, while too high humidity might produce condensation

Video Monitoring

Video monitoring is a part of environmental monitoring. It is a detective security control that could be used to monitor the parking lot as well as the datacenter to verify that neither confidential data nor equipment is being removed

2.7 Disaster Recovery

Disaster Recovery Elements

Components of disaster recovery include backup and backout contingency plans or policies. Factors to be considered include backup plans, and redundancy and fault tolerant measures that aid high availability. Recovery is facilitated by cold, warm or hot sites. Selection among these three types of recovery sites is driven by the mean time to restore, the mean time between failures, recovery time objectives and recovery point objectives.

Backup/Backout Contingency Plans or Policies

In the event that Plan A fails have a pre- conceived and viable Plan B. In the event the weekend datacenter upgrades fail, have a backout plan to undo any changes.

Backup Execution and Frequency

Backup types include full, differential, and incremental. Data deduplication reduces the size of backups, the time to backup, and the time to restore. Backup tape rotation schemes include Grandfather, Father, Son and Tower of Hanoi. One copy of a backup should be stored onsite for quick recovery. Another copy of a backup should be stored offsite away from the main site for disaster recovery.

Redundancy and Fault Tolerance

Redundant measures includes redundant circuits, RAID, clustered servers, network load balancing, mirrored memory, redundant power supplies, and redundant ISPs. These measures increases fault tolerance and remove single points of failure.

High Availability

Five 9's is nearly perfect uptime so that a system might only be down for five minutes a year or just one second a day. This would require automated responses to equipment failure.

Redundancy and fault tolerance foster high availability. However adding too many components to an overall system design adds complexity with more failure points.

Cold Site, Hot site, Warm Site

A cold site is an alternate location with no data and limited if any equipment with which to initiate recovery. It includes electrical and network connections and is the most cost effective. A warm site describes a semi-operational site that in the event of a disaster, IT operations can be migrated. It provided a building and network equipment but not current application data. The highest level of availability is provided by a hot site that has full equipment and current data.

Recovery Metrics and Goals

Recovery metrics and goals include mean time to restore, mean time between failure, recovery time objectives, and recovery point objectives. A high mean time between failure and a short mean time to restore is ideal. Recovery point objectives describe the acceptable amount of data loss measured in time. Depending on business requirements, recovery time objectives and recovery point objectives will dictate the use of a hot, warm or cold site. A hot site can be online in an hour or so, while a warm site would take a day or two, and a cold site might take a month.

2.8 Confidentiality, Integrity and Availability (CIA)

CIA Elements

The parts of CIA are confidentiality, integrity, and availability.

Confidentiality

Confidentiality is protection from unwanted disclosure. Confidentiality is the primary concern of governments in terms of data security. Confidentiality is preserved by strong authentication, strong encryption, ACLs, least privilege, need to know, and sanitization of retired computer systems. On the other hand, items that could compromise confidentiality include USB drives and spyware.

Availability

Availability is the continuous operation of computing systems and networks. Redundancy and fault tolerant measures such as RAID and clustered servers increase availability. A virtualization farm increases availability. Threats to availability include DOS and DDOS attacks, and attacks against HVAC. Vulnerability scanning does not affect availability like penetration testing

Integrity

Integrity is the concept that addresses the threat of data being modified without authorization. Integrity is provided by a hash and input validation. A forensic image of a computer's memory or hard drive should be run through a hash such as SHA256 or SHA512. Finally, Kerberos centralizes file integrity protection.

Threats and Vulnerabilities

3.1 Malware Types

Malware Types

Major categories of malware include adware, viruses, worms, spyware, rootkits, backdoors logic bombs, and botnets.

Viruses

A virus attaches itself to an executable file. You have to do sometime, such as download an open an attachment, to be infected. A viruses' mission is self-replication, so it spreads from file to file within a system. Cell phones with network access and the ability to store data files are susceptible to viruses. Antivirus software gets rid of viruses and other malware. Antivirus software definition files should be continually updated.

Worms

Worms are self contained programs. They can spread by network shares with no user interaction. As a result, worms spread faster than viruses. They can email a copy of themselves to everyone in the address book of an infected computer.

Rootkits

Rootkits are suspicious system-level kernel modules which modify file system operations They are characterized by hooking processes and erasing logs. Hooking process hide themselves from discovery. A hooked process would be found in RAM. Malware scanners may not be able to defeat a root kit that is operating at a higher privilege level.

Trojans and Backdoors

A backdoor is an alternate/unsecured entry point to an application or computer. Programmers might create a backdoor to gain reentry to a crashed application. An example of a back door would be a port that is left open in order to facilitate access at a later date. A Trojan is seemingly harmless program with a malicious hidden payload. It can also be categorized as a malicious program that compromises system security by exploiting system access through a virtual backdoor.

Logic Bombs

A logic bomb is malicious code that is triggered by a time, date, or event. For example, a disgruntled employee inserts additional code into the payroll system which will activate only if he is dismissed. For example, at midnight on January 1st, an administrator receives an alert that all servers are unreachable. Logic bombs are virtually undetectable until triggered.

Botnets

A botnet is a large group of infected computers/bots/zombies that have been taken over by hackers. An indication of a botnet might be several PCs that are running extremely slow all of a sudden, and are opening a large number of connections to the same unknown destination. Generally bots communicate with the zombie master using RC. Firewall logs

should be reviewed to discover botnet activity. A DDOS is an attack launched from multiple zombie machines in attempt to bring down a service or network.

Adware

Adware pops up advertisements. For example, a user who shops online for a new car now receives popups advertising that car. Adware is often bundled with freely downloaded software. After installing the software, random windows might open and close. A popup blocker stops most adware

Spyware

Spyware secretly collects information about users. Spyware negatively affects confidentiality. Spyware can slow down a PC. Tracking cookies and browser history can be used by spyware.

Ransomware

Ransonware is malware that extorts users to pay a ransom to decrypt their data, hard drive, or source code. For example, an attacker that encrypts a users documents and demands payment to decrypt them.

3.2 Attack Types

Attack Types

Major attack types include man-in-the-middle, DDoS, DoS, replay, smurf attack, spoofing, spam, phishing, spim, vishing, spear phishing, xmas attack, pharming, privilege escalation, malicious insider, threat, DNS poisoning, ARP poisoning, transitive access, and client-side attacks.

DOS and DDOS Attacks

A DoS attack from one computer or a DDoS attack from multiple computers attempts to make a computer or network unavailable to legitimate users by consuming resources such as network connections. An example of a DDOS would be a large amount of transmissions from multiple external computers to the web server, which is now inaccessible to users.

SYN Flood, Smurf, & Xmas Tree Attacks

SYN Flood is a DDOS attack in which multiple external hosts start but do not finish the three way TCP handshake exhausting the half open connection queue. Smurf attacks are a DOS attack in which the attacker impersonates the IP address of the victim and pings the subnet broadcast address. Xmas tree attacks set every option for the protocol in use, lighting it up like a Xmas tree. This consumes resources and can be used in a DOS, or in can be used to do stack fingerprinting in which the target OS is identified

Spoofing and Man-in-the Middle Attacks

Attackers can spoof the source IP address, the MAC address, or a Web site. URL spoofing is phishing

If the IP address is spoofed for the purpose of impersonation, then this is a man-in-the middle attack

The attacker monitors the packets, guesses the sequence number, knocks out the victim with a SYN attack and injects his own packets, claiming to have the address of the victim

Replay Attacks vs. Man-in the Middle Attacks
Replay attacks capture and then replay at a later time or date the authentication credentials. Man-in-the-middle attacks take place in real-time. SSL certificate warnings might indicate a man-in-the-middle attack. A replay attack might capture valid wireless traffic for later retransmission to discover the encryption key. The attacking computer will have large network traffic dump files

DNS Poisoning, Pharming and ARP Poisoning
DNS cache poisoning inserts false information in a DNS name server's cache. Pharming redirects Web site traffic to a spoofed Web site, by changing the DNS records, DNS cache, or the hosts file. In ARP poisoning an attacker responds to an ARP broadcast for the victims MAC address with the MAC address of the hacker

Phishing, Spear Phishing, Whaling and Vishing
Phishing attempts to acquire sensitive information by masquerading as a trustworthy entity. Spear phishing targets select groups of people with something in common. Whaling is targeted phishing of senior executives and other high profile targets. Vishing is phishing over the phone.

SPAM, SPIM, & SPIT
SPAM is unsolicited advertising via email. SPIM is SPam over Instant Messenger. SPIT is SPam over Instant Texting. The best location for a spam filter is in front of the mail relay server. The SPAM folder settings should be checked if a user is not able to receive email from a specific user.

Malicious Insider Threat and Privilege Escalation
Insiders often do more damage that outside hackers. WikiLeaks is an example of this. Intrusion Detection/Prevention Systems also monitor/block inside attacks. Auditing is also helpful
In privilege escalation at attacker with access to a user account exploits a bug or configuration error to gain elevated privileges.

Transitive Access
In transitive trust attacks the hacker probes for and attempts to compromise the weakest link in a chain of trust. For instance if a small supplier has access to a extranet for a large company, the attacker will attempt to socially engineer the weakest employee at the small supplier.

Client-Side Attacks
Web client-side attacks target your browser. A modern and patched browser should be used
Security settings should be set to a high level. Pop-up blockers should be used. Unsigned Java and Active X controls should be blocked. Privacy setting should be set to block third party cookies. Where possible HTTP and/or secure cookies should be used. The browser history should be set to automatically erase itself. Unknown browser helpers should be disabled

3.3 Social Engineering Attacks

Social Engineering Attack Types
Social engineering attacks include shoulder surfing, dumpster diving, tailgating, impersonation, hoaxes, whaling and vishing

Shoulder Surfing
Shoulder surfing is looking over someone's shoulder to view confidential information. It is mitigated by users being aware of their surroundings, turning monitors away from doors and windows, password protected screen savers, screen filters, a clean desk policy, and announcing escorted visitors. Shoulder surfing can occur within an office without the use of technological tools.

Dumpster Diving
Dumpster diving involves sorting through the trash in a dumpster to discover information to be used in a subsequent attack. Countermeasures against dumpster diving include sanitizing confidential materials by means of shredding, burning, pulverizing, degaussing, etc. Dumpsters should also be placed in secure areas.

Tailgating
Tailgating is following closely behind an authorized user to gain unauthorized access to a secured area before the door is closed. Countermeasures to tailgating include mantraps, security guards, and user education.

Hoaxes
Hoaxes are falsehoods that convince a user to harm their own computer or their or their organization's security posture. Suspected hoax emails to users should be forwarded to administrators and not to other users. Administrators should check out hoaxes at antivirus websites. Hoaxes can do as much damage as viruses if users are tricked into damaging their own computer.

Whaling
An example of whaling is a convincing, well-researched email attack sent to the company's Chief Executive Officer (CEO). The research makes the email appear to be legitimate. For instance, it could be very similar to an invoice from a supplier. The potential windfall for the attacker is greater.

Vishing
Vishing is Voice Phishing. It leverages VoIP. With VoIP, Vishing attempts can be made without a toll charge from anywhere in the world. Individual have more trust in the party on the other end of the phone line than they do with emails. Caller ID can be spoofed. Vishing can employ a variation of the Nigerian money scam in which the victim is told that a relative left them a large sum of money.

3.4 Wireless attacks

3.4 Wireless Attacks

Wireless attacks include rogue access points, interference, evil twin, war driving, bluejacking, bluesnarfing, war chalking, IV attacks, and packet sniffing.

Rogue Access Points and Evil Twins

A rogue access point is an unauthorized wireless access point that is used to gain access to a secure network. Rogue access points can allow unauthorized users access the company's internal networks

An evil twin is a duplicate access point that has been created to allow a hacker to conduct a man-in-the-middle attack.

Interference

RFI and EMI is eliminated by fiber optic cabling. RFI and EMI are mitigated by shielding, coaxial and STP cabling, and using conduits. Cable runs should avoid sources of interference such as running parallel to electrical lines or close to florescent lights. WiFi interference could be caused by cordless phones, microwaves, and using the same channel as a nearby access point.

Bluejacking, Bluesnarfing, and Bluebugging

These exploits use Bluetooth. Bluejacking pops up unwanted messages on a smart phone. Bluesnarfing is more serious because it allows total access to a smart phone including any data such as an address book and emails. In Bluebugging the attacker can also monitor a smart phone user’s conversation and camera.

War Driving and War Chalking

In war driving a driver searches for Wi-Fi networks using a portable computer or smart phone. War driving is a reason why wireless access points should not be placed near a building's perimeter. In war chalking the location and specifics of wireless access points are documented by nearby chalk marks. It is randomly attempting to connect to wireless network access points and documenting the locations

IV Attacks and Packet Sniffing

The initialization vector (IV) is a semi-random value factored with the encryption key. Longer and more random IVs provide more security. WEP only uses a 24 bit IV. WEP uses an RC4 key that can be discovered by packet sniffing on plain text initialization vectors. Packet sniffing can also discover passwords and other data sent in cleartext by protocols such as FTP, Telnet, PAP, SNMPv1 and v2.

3.5 Application Attacks

Application Attack Types
Application attacks include cross-site scripting, SQL injection, LDAP injection, XML injection, directory traversal/command injection, buffer overflows, zero day attacks, attacks using cookies and/or attachments, malicious add-ons, session hijacking, and header manipulation.

Buffer Overflows
A buffer stores data and instructions. Another name for a buffer is heaps for data and stacks for instructions. An early buffer attack is a NOOP sled. Measures to protect against buffer overflows include input validation, patching, and the no-execute bit of Data Execution Prevention. DLP is a feature of modern CPUs that segregates areas of memory into data and code

SQL, XML, & LDAP Injection
SQL/DLL injection is insertion of bogus information into a database. Stored procedures can be used for SQL injection. XML injection compromises the logic of an XML application or service. LDAP Injection exploits web based applications that construct LDAP statements based on user input. Input validation, secure coding practices and patching are defenses for all of these injection techniques.

Directory Traversal
A directory traversal exploits insufficient validation of user supplied file names so that characters representing "traverse to parent directory" are parsed. The goal is to access a file that is not intended to be accessible such as a password file or other confidential data.

Command Injection
In command injection an attacker modifies dynamically generated content on a Web page by entering HTML code into an input mechanism, such as a form field. Commands are executed with the same privileges and as those of the application. A vulnerability that might allow command injection is a lack of input validation for forms, cookies, and HTTP headers

Zero Day Attacks
A zero-day attack exploits computer vulnerabilities that are hereto unknown so that a patch does not exist. Anomaly based IDS/IPS and antivirus programs that look for anomalies are best are detecting/preventing zero day attacks.

Cookies
Cookies are small text files that pass information between Web pages, such as a shopping cart
Tracking cookies and browser history are used by adware. Third party cookies are from advertisers and should be blocked in your browsers privacy settings. Secure cookies and HTTP cookies protect privacy.

Attachments
Only email attachments from trusted senders should be downloaded. Before opening, attachments should be scanned both by an email gateway and the user. If users can use personal webmail to upload attachments then confidential corporate documents can be pilfered. Data Leak Prevention policies would not allow the use of personal webmail.

Malicious Add-Ons
Malicious add-ons are browser helpers. They may include adware or spyware. In general, anti-spyware programs will not remove them. Unsigned browser helpers should be removed. In Internet Explorer this is accomplished in Internet Properties, Programs, Manage-Addons

Session Hijacking
Session hijacking is the hijacking/reuse of a magic cookie used to authenticate a user to a remote server
So, authentication cookies are exploited in session hijacking

Header Manipulation
TCP and/or HTTP headers are changed in header manipulation. TCP headers have flags such as URG, ACK, PSH, RST, SYN, and FIN. So flags are specific to header manipulation. HTTP headers can also be changed so that malicious data is passed to a vulnerable web application.

3.6 Attack Mitigation and Deterrence

Attack Mitigation and Deterrence Measures
Attack mitigation and deterrence measures include defense against manual bypassing of electronic controls, proactive monitoring of system logs, strong physical security, host and network hardening, port security, a strong security posture, implementation of reporting procedures, as well as detection and preventive controls.

Manual Bypassing of Electronic Controls
Skilled intruders can bypass/disable contact switches, cyberlocks, motion detectors, pressure pads, glass break sensors, and other alarm components. You see this on TV and in movies all the time
Physical detective and preventive systems should updated on a regular basis with the latest countermeasures. Information about protective measures and systems should be kept secret

Specific Logs
Event viewer contains system, security, and application logs. The system Log contains information on system startup, service startup, time changes, and backups. The security log has auditing information
The application log contains events that are logged by applications. Review DNS logs for failed zone transfers and attempted zone transfers to an unknown host. Review DNS logs to reveal who has been querying information about a company's networks. Look at DNS logs for DNS poisoning as shown by requests for non-existent sub-domains. Also review DNS logs to reveal names and IP addresses of all websites visited by employees. To verify if internal web servers are redirecting traffic to a malicious site, review DNS records. Review access logs for brute force attacks against a local administrators account. Review access logs to determine which user inadvertently shut down the company's web server. Review access logs on the server and workstation to reveal who deleted a file. Review access logs if a departmental spreadsheet will not open. Review security logs for user logons and logoffs Only security administrators should have access to the logging server. Logs should be hashed, read-only, or append-only. Review firewall logs for blocked processes or ports if a new software application cannot communicate. Review firewall logs for zombie activity. Review firewall logs if one of the web servers has stopped responding to web traffic. Review IDS/IPS and honeypot logs for intrusions. Review IDS/IPS log for a NOOP sled that indicates a buffer overflow attack. If the CEO can't get to a Web site, review the content filter logs. Review physical access logs for staff members have accessed an authorized area.

Monitoring System Logs
Logging should collect enough information to reconstruct an attack in order, so clocks should be synchronized between servers. This improves forensic analysis of logs. All auditing/logging functions should not be turned on or there will be too much information to review. Log shipping copies logs to a centralized log server using a service such as SYSLOG. This centralized logging helps protect logs from compromise. Only security administrators should have access to the logging server. Logs should be hashed, read-only, or append-only. Finally, erasing logs is a trait of a rootkit.

Physical Security
Physical security includes hardware locks, mantraps, video surveillance, fencing, lighting, as well as proximity and badge readers. Create an access list for an existing badge reader so it

will regulate entry to a secure area. An example of physical security would be a construction of a single heavily fortified entrance to the server room. Cable locks are another example of a physical security control.

Hardening

Hardening includes disabling unnecessary services, protecting management interfaces and applications, password protection, disabling unnecessary accounts, and applying the latest patches. Web servers should be placed in a DMZ after hardening the OS. Web servers should not be a member of a domain so if a Web server is compromised the domain is not.

Reporting

Reporting includes alarms, alerts, and trends. With a constant system changes, managing IT security for servers, workstations, laptops, firewalls, routers, switches and firewalls is extremely difficult to manage without a proactive automated approach. Several third party enterprise management systems enable real time monitoring and reporting of significant security events.

Detection Controls vs. Prevention Controls

Detective security controls include CCTV, facial recognition software, sign in logs, and routine security audits. Preventative physical security controls include an access control system, an armed guard, a mantrap, bollards, and a fortified entrance

Security Posture

Security posture includes initial baseline configuration, continuous security monitoring, and remediation. An initial baseline allows an anomaly detection system to evaluate traffic properly

A denial-of-service attack can be detected by system resource monitors and baselines. The baseline should be updated whenever software is upgraded on a production system. A performance baseline might be referenced to determine if a server is functioning abnormally. Post attack cleanup, the systems performance should be compared to the configuration baseline. A performance baseline will allow detection of a DDoS. If outdated/vulnerable software is deployed on new computers then a secure new configuration baseline should be established for the images. The configuration baseline should be updated after deploying a new service pack. A security template is used to both deploy and reapply baseline security configurations.

3.7 Attack Assessment Tools

Attack Assessment

Attack assessment tools include vulnerability scanning tools, and application that aid in risk calculations. Assessment techniques and categories will also be discussed.

Vulnerability Scanning

A vulnerability scanner is an application that checks computers and networks for weaknesses such as missing patches or misconfiguration. Vulnerability scanners can be used to test the security of a network for a wide range of problems without disrupting operations. A vulnerability scanner is the most commonly used tool to audit a network for

security compliance. A vulnerability scanner could determine if a new device has any known issues with applications.

Tools
Examples of a comprehensive vulnerability scanners include Nessus and the MBSA. Complimentary security assessment tools include port scanners, network mappers, and password crackers. Such as John the Ripper as well as Cain and Abel. Port scanners would show if vulnerable ports are open and could fingerprint/determine the operating system being scanned.

OVAL
The Open Vulnerability Assessment Language (OVAL) was created to standardize the security assessment process and the feed results into a standardized database. OVAL is the most uniform standard to rate the risk exposure of vulnerabilities on a network. OVAL was developed by the MITRE Corporation for Homeland Security and it is based on XML.

Risk Calculations
Risk is equal to the probability that a threat will exploit a vulnerability times the cost of the asset.
Risk = threat x vulnerability x cost of asset. The main difference between qualitative and quantitative risk assessment is that quantitative is based on calculations while qualitative is based on subjective ranking.

Assessment Types
Assessment types include risks, threats and vulnerabilities. Not all vulnerabilities can be exploited by threats. Penetration testing proves that a threat can exploit a vulnerability

Assessment Technique
Assessment techniques include code review, determining the attack surface, network and security architecture review and design reviews. Design review takes place at software development milestones before proceeding to the next phase. The most effective method to provide security for an in-house created application during the software development life cycle (SDLC) is to explicitly include security gates at important milestones. Code review is a thorough review of computer source code after its release. It fixes vulnerabilities overlooked in initial development. An attack surface review would look at limiting the number of entry and exit points for applications and limiting the privileges of APIs used by those applications. A security architecture and design review would determine if controls such as firewalls and NIPSs could be bypassed.

3.8 Penetration Testing vs. Vulnerability Assessment

Penetration Testing vs. Vulnerability Assessment
Topics covered include penetration testing, vulnerability scanning, as well as black box, and white box testing.

Penetration Testing

Penetration testing is more thorough but more disruptive than vulnerability scanning in that it also includes social engineering, buffer overflows, and active testing of physical security. Penetration testing actively tests security controls on a system. Penetration testing exploiting successive vulnerabilities to bypass security controls. Penetration testing should only be conducted after obtaining express written authorization as it actively tests security controls and can cause system instability. An advantage of penetration testing over vulnerability testing is that it proves that a system could be compromised.

Vulnerability Scanning

Vulnerability scanning is a passive attempt to identify weaknesses. If users report corrupted data after a recent patch update, then vulnerability scanning should be used to identify the cause. Vulnerability scanning vice penetration testing should be used when assessing a network containing resources that require near 100% availability.

Black Box, Gray Box, White Box

The color of the box is determined by what a penetration tester knows about a network before testing. In black box penetration testing the penetration tester has no prior knowledge of the network. In grey box penetration testing the penetration tester knows what a user knows. In white box penetration testing the penetration tester is given administrative access. Black box is the most common type of penetration testing. A black box assessment of an application is one where the security assessor has no access to the application's source code and development documentation. Another name for fuzzing proprietary software is black box testing. In fuzzing, random inputs are generated to see if they can compromise an application or system.

Application, Data and Host Security

4.1 Application Security

Application Security Concepts

Concepts include fuzzing, secure coding, cross-site scripting prevention, cross-site request forgery (XSRF) prevention, application configuration baselines, application hardening, and application patch management.

Fuzzing

A fuzzer/fault injector is an application that discovers security vulnerabilities by sending random input strings to a program. A vulnerability is discovered if that input results in an exception, crash or server error. This fuzzing/fuzz testing discovers vulnerabilities to buffer overflow, DoS, SQL/DLL/LDAP injection, XSS, and format string attacks. The format string attack causes an application to interpret an input string as a command.

Secure Coding Concepts

Exception handling takes care of special conditions that change the normal flow of program execution. Code walkthroughs and software testing can catch more exceptional conditions such as bad input to functions and memory and data errors. An attacker creating errors will get responses from exception handling that can be used to determine parameters such as the type of operating system and the type of database. Poor exception handling creates vulnerabilities to many attacks such as buffer overflows, XSS, and DOS. Poor error handling could cause data leakage from web based applications. Input validation insures that only valid data can be entered into a form or application. Input validation has not been done properly if a user entering improper input is able to compromise the integrity of data.

Cross-Site Scripting (XSS) Prevention

In Cross-Site Scripting malicious browser scripts are injected when a user fills out a form or clicks on a link at a trusted web site. The scripts can access any browser information such as Web site passwords. XSS example: <script>source=http://evil.com/evil.js</script>
XSS can be mitigated by input validation. For instance preventing the use of HTML tags

Cross-Site Request Forgery (XSRF) Prevention

While XSS exploits the trust a user has for a Web site, XSRF exploits the trust that a Web site has for a browser. Unauthorized commands are transmitted from the browser. An example of XSRF is harvesting passwords from the web browser's cache. The attack works by including a link or script in a page that accesses a secure site to which the user has been previously authenticated. One preventative measure is a synchronizer token pattern which generates random challenge tokens. Another preventative measure is double submitted cookies in which the session ID cookie is sent first as header value, and second as a hidden form value

Application Configuration Baseline

Application configuration baselines ensure a secure initial configuration for programs. This would include the version, any patches, and permissions on the application. The application would be hashed to make sure that it has not been modified. There might be a hash rule which specifies that only approved hash versions of applications will be enabled.

Application Hardening Methods

In process spawning control the application loses the ability to launch another executable. Executable files protection stops the application from modifying executable files. In system tampering protection the application is only allowed to modify necessary registry keys, and is blocked from modifying system files.

Application Hardening Examples

In application hardening a database administrator could be required to manually change the default administrative password, remove a default database, and adjust permissions on specific files. Application hardening was missing from operational procedures if a penetration test reveals that database servers were compromised with an account with a default password.

Application Patch Management

Operating systems, browsers, and applications should be patched. Windows Update patches only the operating system, while Microsoft Update also patches the browser and other applications such as Microsoft Office. Patches should be only be applied to production systems after vetting them in a test environment that duplicates the production environment.

4.2 Host Security

Host Security Elements

Host security elements include operating system security, protection from malware, performing patch management, enforcing strong hardware security, as well as robust host software baselining, protection of mobile devices, and secure implementation of virtualization.

Operating System Security Measures

Security measures include using a contemporary OS and applying the latest patches once they have been tested. Other protective measures consist of the usage of personal firewalls, HIPS, and antivirus. Measures that bolster security include closing unneeded ports and protocols as well as limiting applications to those necessary, changing system defaults including passwords, disabling remote administration, limiting physical access, setting strong passwords and account lockout policies, securing file systems and the registry with limited user permissions, using EFS, and whole disk encryption, as well as creating and enforcing a security baseline with tools such as Security Configuration and Analysis.

Anti-Malware

Anti malware software includes the following programs / program features: anti-virus, anti-spam, and anti-spyware, and pop-up blockers. The security applications that should be used by traveling employees include: anti-spam, a personal software firewall, and antivirus.

Antivirus
An enterprise antivirus suite should be deployed that has a centralized management station to deploy the latest antivirus definitions, and which also scans email attachments at the email gateway. Antivirus software and IDS/IPS require frequent signature updates. If a user does not have the latest antivirus definitions, they might discover after a long business trip, that their laptop is having performance issues and unauthorized emails are being sent out from their laptop. To aid in preventing the execution of malicious code in email clients spam and antivirus filters should be used. Use only tested and approved antivirus software. If you get a pop-up message stating that antivirus software should be downloaded from the site to clean the infection. Do not do this. This is an example of social engineering. In general, antivirus software can detect and delete downloaded malware. However, antivirus software may not be able to detect malware that uses virtualization techniques as it may be running at a more privileged level than the antivirus software.

Anti-Spam
Spam is unwanted email with advertising. An anti-spam solution prevents unsolicited email messages from entering the company's network. SPAM can also be blocked at the email gateway. An organization should close open relays on their email servers so that they do not send spam and get on a real-time black hole list. The best place for an anti-spam filter is in front of the mail relay server. If a user cannot find a legitimate email, he should check his junk email settings and folder.

Anti-Spyware
Spyware transmits PII from your computer to Internet sites without your knowledge. Spyware negatively affects confidentiality. Spyware might be the issue, if a user has recently updated their antivirus, and now, after accessing several different Internet sites, their computer is running slow
Spybot Search and Destroy is a free, but robust anti-spyware scanner. It can be used without affecting antivirus software.

Pop-up Blockers
Pop-up blockers protect against non-malicious but irritating malware. Pop-up blockers mitigate the security threat of adware. A pop-up blocker would stop ads from appearing in new windows for sites that are not safe for work.

Host-Based IDS/IPS
HIDs do logging and alerting on a host. HIPs are like an antivirus on steroids. They can log off a user, disable an account, stop a write to the registry, and stop a process or application from launching. A HIDS would alert an administrator if a specific server within the company's network is being attacked. A HIPS would also block that attack.

Host-Based Firewalls
A host-based firewall (also called a personal or software firewall) is a program that protects a single Internet-connected computer from intruders. They are particularly useful when users have a continuous DSL or cable modem connection. It would give remote users the needed protection from outside attacks, as well as help prevent a system from being fingerprinted by port scans. It is an efficient way to secure a single laptop from an external attack. A software firewall can restrict a computer from receiving network traffic, and can mitigate port scanning attacks from the Internet. It stops attackers when they are outside

of the company's internal network. For example, a personal firewall would explain why an employee keeps getting pop-ups from a program on their computer stating it blocked an attacking IP address.

Patch Management

A patch fixes bugs in their programs, addresses security problems, or adds functionality. A hot fix is an unscheduled release of a patch that fixes a critical issue such as a vulnerability. Hot fixes are not fully tested. A service pack is a fully tested set of patches. It updates a network machine with a number of vendor fixes concurrently. An enterprise patch management system should be used. Patches are downloaded to a patch management server, tested, approved, and pushed out to client machines. The last step in patch management is auditing to ensure patches have been installed on all workstations. A personal firewall might block patch installation.

A service pack ensures that all major software revisions have been installed on a critical computer. All current service packs and hotfixes should be re-applied if a computer was reimaged. A hotfix should be released quickly outside a normal update cycle if a security flaw allows backdoor access into the system

Virtual servers and their hosts should have the latest service packs and patches applied. Patch management includes mitigating security risks by updating and applying hot fixes. Outdated versions of software would indicate weak patch management. Patch management helps ensure that there are no security holes in the OS. It would apply various fixes on different applications and protects against operating system security flaws. Documenting the security assessment and decision in patch development means that the reason for patch development is documented and that security goals are met. Regression testing and deployment are part of patch development and deployment. In regression testing the software developer of a new patch tests it before releasing it to make sure that it does not negatively affect the patched application or OS. Patch management ensures that all systems have the most up-to date software version available. Disseminating a patch management policy would give administrators a clear timeline of when patches must be installed. The three major activities of patch management are determining which patches are needed, applying the patches, and auditing for the successful application of the patches.

Hardware Security Components

The elements of robust hardware security include a locked server room, locking cabinets, a safe, cable locks, security screws, and computer case intrusion detection.

Host Software Baselining

A host software baseline is a secure starting point. Baselining software includes MSBA and Nessus. Whenever major changes to software are made the baseline should be adjusted. A security template is used to both deploy and reapply baseline security configurations. Another way to apply a software baseline is disk imaging.

Mobile Device Security Features

Mobile device security features include screen lock, strong passwords, device encryption, remote wipe/sanitation, voice encryption, GPS tracking, and antivirus.

Mobile Device Security Examples

A mobile device should erase itself after a set number of invalid password attempts. Voice encryption should be implemented on a mobile phone to help prevent a conversation from being captured. Device encryption should be enforced on mobile devices to prevent data loss from stolen devices. Remote sanitization would mitigate the risk of stolen classified mobile devices. Screen lock will prevent viewing the home screen on a mobile device if left momentarily unattended.

Virtualization

Virtualization reduce the footprint of resources that must be protected. Both the host and guest OSs should be patched. The guest OS has the same security requirements and the host OS. A single physical server hosting multiple virtual machine is a single point of failure. Multiple physical hosts increase availability and fault tolerance

4.3 Data Security

Data Security Elements

Components of data security include data loss prevention (DLP), data encryption, hardware based encryption devices, and cloud computing.

Data Loss Prevention (DLP)

DLP systems monitor and protect data whether it is at rest, in use, or in motion. DLP techniques include content inspection, and analysis of transactions within a centralized management framework. DLP goals include detection and prevention of unauthorized use of confidential information. Install a network-based DLP device to reduce the risk of employees emailing confidential data outside of the company.

Data Encryption

Full disk using Bitlocker, two partitions, and a TPM. Database encryption using transparent data encryption (TDE) in SQL Server 2008, or third party encryption products. Individual files and folders using EFS. Removable media using WinMagic's SecureDoc, McAfee Endpoint Encryption, or Bitlocker in Windows 7, or Windows Server 2008 R2. Mobile device encryption – elliptical curve cryptography (ECC) has the lowest processing requirements and extends battery life.

Hardware Based Encryption Devices

TPM - Securely generates encryption keys. Its remote attestation feature creates a hash the hardware and software so that the TPM will not work if moved to another computer. HSM – Safely store asymmetric key pairs and offload cryptographic processing from application servers. USB encryption – Is essential as USB sticks are easily lost or stolen. Built-in hardware encryption is more secure and faster than software encryption. Hard drive – Asymmetrical encryption such as ECC is the strongest encryption for a hard drive. Symmetrical encryption such as AES is the most common and the quickest. A HSM is the most secure way of storing keys or digital certificates used for encryption/decryption of SSL sessions. A HSM is a removable device that may be used to encrypt in a high availability clustered environment. A TPM is a hardware chip that stores encryption keys. It is used in conjunction with software-based encryption and enhances platform authentication by storing unique RSA keys and providing cryptoprocessing. It would prevent a user from

losing the encryption key to their laptop hard drive

Cloud Computing

Cloud computing outsources some of or virtually all datacenter features to a service provider

It is elastic, on-demand, and can save money. But the company loses full control over their data

Blended systems and data add complexity which can reduce security. A 2011 service interruption at Amazon Web Services raised doubts about cloud computing.

Access Control and Identity Management-

4.4 5.1 Functions of Authentication Services

Authentication Services
These include RADIUS, TACACS, TACACS+, Kerberos, LDAP, and XTACACS

RADIUS
RADIUS is Remote Authentication Dial-in User Service. The Radius Server is the AAA service provider. AAA stands for Authentication, Authorization, and Accounting. The RADIUS Client is the network access server or device (i.e. wireless router). RADIUS is scalable and interoperable. RADIUS and TACACS+ are the most common AAA servers.

TACACS and XTACACS
TACACS stands for Terminal Access Controller Access Control System. XTACACS has additional support for accounting and auditing. TACACS and XTACACS were primarily used on Unix / Linux systems, and routers. Both are from Cisco and supports a wide range of protocols. RADIUS and XTACACS use UDP. TACACS can use TCP or UDP. TACACS+ uses only TCP.

TACACS+
TACACS+ is an improvement to , but not backward compatible with TACACS or XTACACS. TACACS+ also supports a robust set of protocols. TACACS+ uses TCP exclusively so it gives immediate feedback on network problems and keeps retrying
It is more secure that RADIUS in that it encrypts the client server security negotiation dialogs. Unlike RADIUS. TACACS+ separates the authentication, authorization, and accounting packets. A reason to use TACACS+ over RADIUS is encryption of all data between client and server. TACACS+ and RADIUS are most likely to be used to centrally manage authentication across network devices. The main difference between TACACS and TACACS+ is that TACACS+ uses TCP while TACACS can use either TCP or UDP. TACACS+ uses multiple-challenge responses for authentication, authorization and audit.

Kerberos

Kerberos refers to the mythical three-headed dog that guards the gates to hell. Its strength is in timed authentication tokens. Kerberos authenticates principals, who can be a user or device, to a realm/domain. The Kerberos Key Distribution Center (KDC) is the equivalent of a DC in Windows. The KDC functions as both an Authentication Server (AS) and a Ticket Granting Server (TGS) In Kerberos the principal is authenticated by the AS and given a session key called a ticket granting ticket (TGT) that is good for a workday When the principal wants to access a resource such as a file server, this request is passed to the TGS that issues an authenticator that is good for only five minutes. This prevents replay attacks. It also follows that the clocks must be synchronized in Kerberos. Centralized file integrity protection is a reason to implement Kerberos over local system authentication. Kerberos uses tickets to identify users to the network. Kerberos is an authentication method that uses symmetric key encryption and a key distribution center. Kerberos is used for authentication in Active Directory. Kerberos uses a trusted third party key distribution center to generate authentication tokens. A user that worked 13 hours in one day might not be able to access the system because the user's ticket has expired. Kerberos can be used to help prevent man-in-the-middle attacks. Kerberos is a method of AAA that is most secure by default.

LDAP

LDAP is Lightweight Directory Access Protocol. LDAP requires TCP/IP and DNS to store information in a hierarchical database for the purposes of single sign-on, management, and security

LDAP information is stored in an inverted tree format, with container objects such as domains, and OUs, while leaf objects such as users, computers, and printers. LDAP based directory services include Microsoft's Active Directory, Novell's eDirectory as well as versions for UNIX and Linux. LDAP injection is an application attack used against Active Directory based systems. LDAP is typical among corporate environments to authenticate a list of employees

5.2 Authentication, Authorization, and Access Control

Authentication, Authorization, & Access Control Topics

These include identification vs. authentication, single factor and multifactor authentication, authorization, biometrics, tokens, ACLs, CAC , PIV and smart cards, as well as the concepts of least privilege, separation of duties, and single sign on.

Identification vs. Authentication

Identification precedes authentication. You would identify someone based on a birth certificate, drivers license, or something they know such as their mother's maiden name.

Asking a user something that others would not know is called identity proofing. In authentication a user employs a digital credential to prove their identity to a system. In non-repudiation the user cannot deny having done something
The process of validating a user's claimed identity is called identification. Identification is applied first when a user logs into a domain. Identification is the process of verifying the user or computer system
Identity proofing includes non-repudiation as well as identification. An example of identification is an organization policy requiring employees to display their corporate badge at all times. Identification and authorization should be finished before access is given to the network. Authentication is the concept applied when a user enters a password to gain authorized access to a system. Authentication has occurred after a user has successfully gained access to a secure system. A stronger form or single factor authentication is something you have such as a CAC card or an RSA token. The strongest form of single factor authentication is biometrics, but this is also the most costly to implement. Examples of biometrics include iris and retina scans, fingerprints, hand geometry, DNA, and scans of the veins in your arm or leg.

Authentication (Single Factor) and Authorization
A subset of biometrics are measurements based on a subjects behavior such as voiceprints and signature dynamics. Another potential authentication factor is location. For instance you might have to be at a workstation in a secure area to have full access to a confidential database. Once you are authenticated you are authorized access to different resources based on your user identity and any group membership
A RSA token provides a rolling password for one-time use. An iris scan is a stronger authentication method than fingerprints, or a smartcard. Biometrics is an example of something the user is. The SAM contains a database of users and passwords used for authentication. If usernames and passwords are replaced with USB security tokens, then this is still single factor authentication.

Multifactor Authentication
When more than one category of authentication is used, this is called multi-factor authentication. Multifactor is considered strong authentication. Using a smartcard and PIN is an example of two factor authentication. Using a smartcard and a physical token is just single factor authentication. A password, retina scan, and a one-time token would constitute a valid three factor authentication system.

Mutual Authentication
Mutual authentication is where the server not only authenticates the user, but the user authenticates the server. MS-CHAPv2 provides mutual authentication. Mutual authentication would identify and defeat a rogue server or evil twin.

Biometrics
A fingerprint reader is the most common biometric reader. Gummy fingers can spoof a fingerprint reader. A retina scan or iris scan is more secure that a fingerprint scan. DNA scans and vein scans of the arm or leg are also hard to spoof. Facial recognition would prove who had entered the datacenter.

Separation of Duties

Separation of duties creates a check and balance. Separation of duties makes social engineering harder in that more than one person has to be compromised. Separation of duties should be implemented to provide a check and balance against social engineering attacks. Separation of duties would be violated if an application programmer at a company also conducts security assessments. Separation of duties is enforced server administrators cannot have access to log servers or permissions to review log files. Separation of duties is implemented if the security manager divides responsibility for firewall and NIDS administration between different technicians.

Single Sign On

A single sign on (SSO) grants access to multiple resources based on a single authentication. Users do not have to remember multiple passwords. In a SSO a user would centrally authenticate to multiple systems and applications against a federated user database. SSO often requires different systems to function together and is complicated to implement in non-homogeneous environments. SSO allows access to multiple systems with a single authentication method. An SSO example is a user logs onto a laptop with an encrypted hard drive. There is one password for unlocking the encryption and one password for logging onto the network. Both passwords are synchronized and the single password only has to be entered once. A SSO is a single point of failure on a network. SSO is the ability to logon to multiple systems with the same credentials. A SSO would be the solution if a company has a complex multi-vendor network consisting of UNIX, Windows file servers and database applications. Users report having too many passwords and that access is too difficult.

Tokens

A security token is a small hardware device that generates unique keys based on time or a counter

Examples are a smart card, CAC card, PIV card, or RSA token. Generally the user must not only have the token, but the PIN. This provides two-factor authentication. Tokens allow a user to have a one-time password and to store longer keys than the user could remember.

CAC, PIV and Smart Cards

CAC stands for Common Identity Card. CAC is a type of Personal Identity Verification (PIV) card. A PIV card is an example of a smart card. CAC/PIV cards are smart cards that store a user's private key. This key is used to authenticate. Smart cards also facilitate encrypting and cryptographically signing email.

Access Control for Files

An ACL allows you to allow or deny permissions. Effective permissions are a combination of user and group permission unless there is an explicit deny. There is an implicit deny for all permission not granted. Share permissions combine with NTFS permission so that only the least permission between the two survives.

ACLs

An Access Control List (ACL) is a list of permissions to a resource. An ACL is a logical access control method that controls network traffic passing through a router to a different network. An ACL would control traffic being routed between networks or network segments in an effort to preserve data confidentiality. An ACL is an authentication methods that is typical among corporate environments to authenticate a list of employees. The ACL entry <deny any any> best represents the concept of implicit deny. A port scanner is a vulnerability assessment tool used to identify weaknesses in a router's or firewall's ACL. An ACL determines if traffic is blocked or allowed. An ACL is a security control that can utilize a command such as <deny ip any any>. A best practice for granting access to resources is adding groups to ACLs and adding users and computers to groups. The ACL should be checked if a user is no longer able to transfer files to the FTP server, and the security administrator has verified the ports are open on the network firewall. The firewall log will reveal activities about an ACL

NTFS Permissions

The key NTFS permissions are full control, modify, read & execute, read, and write.

Share Permissions

The share permissions are full control, change, and read.

Mandatory Access Control (MAC)

Access is based on security labels such as confidential, secret, and top-secret. Access is granted to individuals after an extensive background investigation by a centralized authority. There are no group privileges. This model is non-dynamic. It is based on a matrix of subject clearances against object sensitivity labels. Subjects also must have a need to know. MAC is a policy that restricts access to objects based on security clearance. MAC allows access associated with the classification of data

MAC allows access control determinations to be performed based on the security labels associated with each user and each data item. A SQL database as well as a router most likely implement MAC. A lattice best describes the Mandatory Access Control model. In Mandatory Access Control users cannot share resources dynamically. Valid access control methods include MAC, DAC and RBAC.

Role Based Access Control (RBAC)

In role based access control, users are added to single roles, and permissions are assigned to those roles. Users get no individual permissions. RBAC is based on user tasks or responsibilities. Typical roles would be Finance, Sales, Research and Development, and Production. RBAC would be ideal for a restaurant with a high turnover.

Rule Based Access Control (RBAC)

An example of rule based access control would be controlling access to a training room so that it was only open to attendees during training periods. Rule-based access control is closely aligned with MAC.

The primary difference between role-based access control and rule-based access control is that one is based on job function and the other on a set of approved instructions.

Discretionary Access Control (DAC)
Access to resources is set and is at the discretion of the owner of the resource. Permissions are set using Windows Explorer. DAC is provided on Windows systems by default. In DAC all objects have an owner, and this owner has full control over that specific object. The flaw in DAC is that uses only the identity of the user or specific process to control access to a resource. This creates a security loophole for Trojan horse attacks. DAC uses Access Control Lists to identify the users who have permissions to a resource. In DAC, users get individual and group permissions, oftentimes from multiple groups

Implicit Deny
In implicit deny, subjects or objects not explicitly allowed are denied access by default. The last and unwritten firewall rule is an implicit deny. Implicit deny is the most secure starting point for a new firewall policy. Implicit deny means that the firewall only permits the specific needed applications to pass through the firewall, and everything else is denied. On a network ACL <deny any any> best represents the concept of implicit deny.

Time of Day Restrictions
Time of day restrictions can be implemented to ensure an employee cannot use the system outside of normal business hours. Time of day restrictions and an ACL should be implemented if a security administrator wants to prevent users in sales from accessing their servers after 6:00 p.m., and prevent them from accessing accounting's network at all times.

Trusted OS
A Trusted OS (TOS) is an OS that provides multilevel security and meets enhanced security requirements. The Common Criteria is the most implemented set of criteria for TOS design and certification. Security Enhanced Linux (SELinux) is a trusted OS implementation used to prevent malicious or suspicious code from executing on Linux and UNIX platforms.

Mandatory Vacations
Some companies such as banks might specify that employees need to take two consecutive weeks of vacation a year so their work can be audited. Implementing a mandatory vacation policy for administrators is a security best practice because of it detects malicious actions by an administrator responsible for reviewing logs.

Job Rotation
Job rotation insures that others are trained and that there is not a single point of failure. An example of job rotation is employees in the accounting department moving between the accounts payable and accounts receivable roles every three months. Job rotation ensures that an employee cannot continue carrying out fraudulent activities

5.3 Account Management

Account Management Topics

These include mitigating issues associated with users with multiple account/roles, account policy enforcement, group based privileges, and user assigned privileges.

Password Policies

These include password complexity, expiration, recovery, length, disablement, and lockout.

Passwords and Account Policy Enforcement

Attacks against passwords include guessing, dictionary, brute force, hybrid, and masked. A dictionary attack can determine whether common words and phrases are being used as passwords on the company server. A hash of passwords is stored on the server. Passwords are cracked by a comparative analysis

A Rainbow Table hashes potential passwords and sorts the hashes for easy comparison. A SALT is a random value appended to a password before it is hashed to defeat a Rainbow Table. A self-service password reset is the most scalable. Short passwords should be protected from password guessing using account lockout. A dictionary attack would determine whether common words and phrases are being used as passwords on the company server. Password crackers include John the Ripper as well as Cain and Able. An administrator should implement a strict domain level group policy if he is concerned that users are not utilizing strong passwords. A username and password is the least secure authentication method. If an attacker wants to crack passwords on a server with an account lockout policy then the password file should be copies offline and then attacked. An administrator should create an additional account without administrative privileges to ensure that he is logging in using least privilege. A password cracker would be most useful for a security technician to run on a single, standalone machine with no network interface to verify its overall security posture. On network devices where strong passwords cannot be enforced, the risk of weak passwords is best mitigated through the use of limited logon attempts. An intruder has gained access to a server and installed an application to obtain credentials. This tool was probably a password cracker. John the Ripper could be used by a penetration tester in a brute-force attack to discover network passwords. Weak passwords are exposed by Rainbow tables. An example of password expiration requirements is forcing users to change their password every 90 days. An example of password length requirements is requiring users to have a password of 16 characters or more. Password recovery is exemplified by allowing a user to perform a self-service password reset. Account disablement is a security best practice when an employee leaves the company. Password complexity is being enforced if users have to use at least ten upper and lower case alpha-numeric characters and special symbols. Letters, numbers, and special characters increase the key space of a password the most. Account lockout has been implemented if several unsuccessful login attempts were made in a short period of time denying access to the user account, and after two hours the account becomes active. The SAM contains a database of users and passwords used for authentication. Set a domain password policy if the administrator needs to require all users to use complex passwords. Clustering is used to distribute the processing effort to generate hashes for a password cracking program. Group policy could enforce the policy that users must use 15 character passwords. An account expiration policy targets employee accounts that have left the company without going through the proper exit process. Ensure that passwords are not named after relatives to mitigate social engineering threats. On domain controllers password complexity be enforced via group policy

An example of password complexity requirements is requiring users to have a password that consists of alphanumeric and two special characters.

Group Assigned Privileges

Implement access based on groups is an account management principle for simplified user administration. A security group can be assigned permissions while a distribution group is only for email. A best practice for granting access to resources is to add groups to ACLs, and add users and computers to groups. If the auditors group needs access to the

applications of three other groups, then add the auditors group to each of those three groups. Viewing the results of a risk assessment should be limited to the information security employees and executive management. The concept of least privilege, required access, and security role should be applied when managing user access with groups To enforce information assurance controls remove unnecessary users from groups with permissions to the resources. Delegation of administration and policy deployment is a best practice when creating groups of user and computer accounts in a directory service.

User Assigned Privileges

Creating individual accounts fosters individual accountability. A best practice for managing user accounts is to notify account administrators when a user leaves or transfers. The user rights assignment policy was violated if a user has more access to a financial application than they should. Conducting periodic user rights audits can help an administrator identity users who can view confidential information. Deny network logon is a best practice relating to non-administrative user rights on a server. Auditing account login would verify the time and date certain users access a server

Cryptography

6.1 Cryptography Concepts

Cryptography Concepts

Key concepts include symmetric vs. asymmetric encryption, block vs. stream ciphers, transport encryption, non-repudiation, hashing, key escrow, steganography, digital signatures, using proven technologies, and finally elliptic curve and quantum cryptography.

Crytography

Cryptography is the study of encryption. Encryption is converting information to a secret format / cipher text. Decryption is conversion back to plain text. An algorithm is a mathematical formula for encrypting or decrypting. A algorithm plus a variable secret key is used to encrypt data. Cryptography supports – confidentiality, integrity and non-repudiation

Symmetric vs. Asymmetric

Symmetric encryption uses the same key to encrypt and decrypt. Other words for symmetric keys are single, same, secret, and session keys. It is the fastest form of encryption, but a unique symmetric key must be securely distributed to each party, so if an ecommerce Web site communicates with a 100,000 customers then they would need to manage and secure 100,000 keys. Asymmetric encryption solves the key distribution problem. It is based on a public and private key pair. The public key is freely distributed and used to encrypt

The private key is kept secret and is used to decrypt. Asymmetric encryption is 100 times slower than symmetric encryption so it is usually used to encrypt a session key and then the session key is used to encrypt the data.

Block vs. Stream Ciphers

Stream ciphers encrypt one character of data at a time. The output is the same size as the input. Stream ciphers such as RC4, are faster than block ciphers, but not as secure. Just about all contemporary ciphers are block ciphers.

Encryption

The main benefit of encryption is confidentiality. Confidentiality protects against unauthorized disclosure of information.

Transport Encryption
Transport encryption covers encryption of data in transit. Examples would be VPNs, SSL, TLS, HTTPS, and SSH. VPN protocols include PPTP, IPSEC paired with L2TP, IPSEC by itself, and SSTP. TLS is stronger than SSL because TLS checks that a certificate belongs to a Web site. TLS could be used to encrypt email in transit between email servers. PGP has a product for voice encryption.

Non-Repudiation
Non-repudiation is the concept that a sender cannot deny sending a message. So if a company inadvertently low-balls a contract, they cannot deny their bid. Non repudiation is provided by a hash

Hashing
A hash takes a variable sized input, runs it through an algorithm and creates a fixed sized output. It is a one-way operation. Single-bit changes in plaintext modify the hash in an unpredictable manner. Hashes provide authentication, message integrity, and non-repudiation. Longer hashes are more collision resistant. A collision is when two inputs provide the same hash.

Key Escrow
Key escrow is storage of cryptographic keys with a trusted third party for later retrieval. For faster key recovery use a local recovery agent. A recovery agent is an alternate user, such as an administrator who can recover lost or corrupted cryptographic keys.

Steganography
Steganography does not encrypt data, it hides it. Data can be hidden using invisible ink, microdots, watermarks, variations in wav files, and variation of the least significant bits of the colors of pixels in an image. Steganography embeds a message within the bits of an image file. Steganography is exemplified by data obfuscation within a data stream. Steganography involves placing plain text data within a picture or document. An example of steganography is website source code containing suspicious numbers of white spaces and non-printable characters at the end of each line of code. If a security administrator is reviewing a JPEG's metadata and hash against an unverified copy of the graphic, then the administrator is looking for steganography.

Digital Signatures
In asymmetric encryption there are four keys: Public key of the sender - used to verify the digital signature of the sender. Private key of the sender – used to create the digital signature. Public key of the recipient - used to encrypt data. Private key of the recipient - used to decrypt data. The private keys are never shared.

Use of Proven Technologies
Some companies have proprietary encryption protocols that they do not share. They seek security by obscurity. This sounds like a good approach, but it isn't, because the encryption protocols are not widely tested. The best approach is the use of field-tested and proven encryption protocols and technologies.

Quantum Cryptography
Quantum mechanics describes the probability that the system is to be found in a given state at a given time by the construct of a quantum wave. Quantum cryptography uses this principle to encrypt, and securely exchange a key (quantum key distribution). Quantum cryptography can perform tasks that are impossible with classical cryptography such as breaking public key encryption and detecting an adversary's interference with a message.

Elliptical Curve Cryptography
Elliptic curve cryptography (ECC) is based on the elliptic curves functions over finite fields. With ECC a shorter key will still be secure. It also requires less processing power so it's ideal

for smart phones as it will yield longer battery life. ECC is the strongest common asymmetrical encryption method
Asymmetrical encryption is stronger (but slower) than symmetrical encryption, so for the strongest encryption of a hard drive, use ECC.

6.2 Cryptographic Tools, Products, and Algorithms

Cryptographic Tools, Products, and Algorithms

These include WEP, WPA, WPA2, MD5, SHA, HMAC, RIPEMD, DES, 3DES, RC4, AES, Blowfish, TwoFish, RSA, Diffie Helman, ECC, one-time-pads, PAP, CHAP, LANMAN, NTLM, NTLMv2, PGP/GPG/SMIME, whole disk encryption, and transport encryption.

WEP vs. WPA/WPA2

Wired Equivalent Privacy is weak, in part because of a short 24-bit initialization vector, and the passphrase is shared by the access point and all stations until it is manually changed. Wi-Fi Protected Access is stronger than WEP because it uses EAP and TKIP. EAP allows stronger authentication credentials such as certificates. TKIP changes part of the encryption key on a minute-by-minute basis

A drawback of WPA is that it still uses RC4, a stream cipher like WEP. Wired Equivalent Privacy is week, in part because of a short 24-bit initialization vector, and the passphrase is shared by the access point and all stations until it is manually changed. Wi-Fi Protected Access is stronger than WEP because it uses EAP and TKIP. EAP allows stronger authentication credentials such as certificates. TKIP changes part of the encryption key on a minute-by-minute basis. A drawback of WPA is that it still uses RC4, a stream cipher like WEP. WPA2 improves on WPA by using AES instead of RC4

802.11i improves on WPA2 by using CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) instead of TKIP. CCMP changes the whole encryption key on a minute-by-minute basis, not just part of the key.

MD5 , SHA, HMAC, RIPEMD

These are all hashes. MD5 is the shortest and quickest, but least secure hash at 128 bits. SHA1 is more collision resistant at 160 bits. Other versions of SHA have 224, 256, 384, or 512 bits, i.e. SHA512

RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest) has a 160-bit key and has performance similar to SHA1. There are also 128, 256 and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320.HMAC is a specific type of MAC function. It uses an underlying hash function over a message and a key. HMAC (Hash-based Message Authentication Code) can piggyback on MD5, SHA, RIPEMD, etc. Its advantage is that it is very fast and compact. It is used for authentication, and message integrity. Its disadvantage is that it cannot be used for non-repudiation. SHA is used to provide a fixed-size bit-string regardless of the size of the input source. MD5 will allow a user to verify that the file is the original.

DES, 3DES, RC4, AES, Blowfish, TwoFish
These are symmetric encryption algorithms. DES is old and only 56 bits. It is usually the least secure, but RC4 can be configured to be less secure. RC4 is the only stream cipher among these 3DES uses three iterations of DES with three keys. It is the slowest. 3DES should be used if AES cannot be used for a VPN due to old equipment. AES256 is the most resistant to brute force attacks. RC4 can be configured as the least secure. AES is capable of providing the highest encryption bit strength. 3DES uses multiple encryption keys to repeatedly encrypt its output. The strongest way to encrypt email is AES. AES competitors include Rijndael and TwoFish. Rijndael won, but TwoFish is still strong
Blowfish is another very strong symmetric algorithm with up to a 448 bit key.

RSA, Diffie Helman, ECC
RSA is an asymmetric algorithms designed to provide both encryption and digital signatures. RSA relies on prime numbers to generate keys. RSA tokens provides a rolling password for one-time use
RSA is a public key cryptosystem. RSA is used to generate keys in PKI. Diffie-Hellman key exchange is most integral to HTTPS. Diffie-Hellman addresses key management. Elliptic curve is best suited for small portable devices such as PDAs and cell phones. Elliptic curve provides the strongest security when implemented correctly. Elliptic curve provides the strongest security for whole disk encryption

One-Time Pads (OTP)
In a one time pad the length of the key is equal to the length of the data. The key has variable offsets for each character. A one time pad is virtually unbreakable. A one-time pad implements a secure key distribution system that relies on hardcopy keys intended for individual sessions. A one time pad is considered an unbreakable algorithm because the key is not reused.

PAP and CHAP
PAP sends the password in the clear and should not be used. CHAP is based on a challenge string from a server that is used by the client to hash the password so it is protected. CHAP also performs random challenges even after the user is initially authenticated. MS-CHAP encrypts the data on the hard drive as well as over the network. MS-CHAPv2 does mutual authentication.

LANMAN, NTLM, NTLMv2
LANMAN was an early and weak, password hash used by Microsoft. It stored the password in the two seven character blocks. NTLM is stronger, but it too should be disabled in favor of Kerberos and NTLMv2. The only reason to use NTLMv2 is for legacy client support, or to support authentication for computers that are not a member of the domain. LANMAN is seen as non-secure based on its ability to only store seven uppercase characters of data making it susceptible to brute force attacks
LANMAN would be in use if a security administrator has discovered through a password auditing software that most passwords can be discovered by cracking the first seven characters and then cracking the second part of the password.

PGP/GPG
These are all secure email programs that provide encryption and digital signing with the following benefits: Confidentiality, integrity, authentication, and non-repudiation. GnuPG is

open source/free email encryption and digital signing software. It features a versatile key management system as well as access modules to public key directories. PGP is Pretty Good Privacy. In PGP there is no central certificate authority. Users create their own PGP certificates. PGP uses a mesh of trust/web of trust/peer-to-peer trust to validate certificates by trusted peers called introducers. It defines its own certificate format. A single certificate can contain multiple signatures. PGP uses a trust system where public keys are stored in an online directory. PGP is a cryptosystem based on the asymmetric encryption method. RSA is PGP based.

PGP Certificate Format
PGP version number, certificate holder's public key, certificate holder's information, digital signature of certificate owner, certificate's validity period, and the preferred symmetric encryption algorithm for the key.

S/MIME
S/MIME certificates best describe a tool used to encrypt emails in transit. S/MIME would be used to send an encrypted email. S/MIME is most closely associated with email

S/MIME Certificate Format
S/MIME uses standard X.509 certificates from a central certificate authority to encrypt and digitally sign messages. The S/MIME certificate fields include the version, certificate holder's public key, the serial number, certificate holder's distinguished name, certificate's validity period, unique name of certificate issuer, digital signature of issuer, and signature algorithm identifier

AES and Email
AES would be the most secure choice for encrypting email

Whole Disk Encryption
EFS would be used to encrypt a folder within a hard drive. To encrypt the whole hard drive a program such as BitLocker would be used. Two partitions are required. The boot partition is not encrypted. For security, the hard drive is locked at boot in case of the following: disk errors, BIOS changes, startup file changes. The hard drive key is stored separately. BitLocker requires a USB flash drive or a TPM. A TPM is a hardware chip that stores and generates encryption keys. A TPM when used in conjunction with software-based encryption, it enhances platform authentication by storing unique RSA keys and providing cryptoprocessing.

Comparative Strengths of Algorithms
Asymmetric algorithms are stronger than symmetric algorithms so ECC is stronger than AES. Among asymmetric algorithms ECC is stronger than RSA or Diffie-Helman. RSA requires a 2048 bit length for strength. AES is stronger than 3DES, but 3DES is a decent alternative. DES is generally weakest, but RC4 can be configured to be the weakest .

Use of Algorithms with Transport Encryption
SSL is the underlying protocol of HTTPS but can be used to set up a SSTP VPN. TLS is stronger than SSL in that it checks that a certificate truly belongs to a web site. IPSec can be the tunnel and the encryption for a VPN, or just the encryption piece when used with L2TP. SSH is for secure remote access and file transfer. HTTPS provides a secure Web site

6.3 and 6.4 Public Key Infrastructure (PKI) Concepts and Implementation

PKI Elements
These include certificate authorities (CAs), certificates, PKI, recovery agents, and the public key.

Certificate Authorities
Certificate Authorities issue keys and maintain the CRL. Optionally they backup the encryption keys
They may have a third party key escrow company handle backup. Typically keys are issued, used, expire, and are renewed. In the case of private key compromise, CA compromise, or problems with a company a certificate can be suspended or revoked. The advantage of a third party certificate authority is that its certificates are trusted worldwide. The disadvantage is that the certificates have a significant cost, particularly when thousand of certificates are required for employees. The advantages of an organization issuing their own certificates are more control and less cost. A company could install the Certificate Services role on Windows Server 2008 and realize these savings. While commercial CA certificates are automatically installed in browsers, a organization would generally use group policy to push out their certificates to their browsers trust list. The CA is responsible for verifying the authenticity of certificate contents.

The Certificate Revocation List (CRL) and the Online Certificate Status Protocol (OCSP)

The CRL should be checked regularly to avoid using compromised certificates. The CRL contains a list of certificates that are compromised and invalid. The main disadvantage of implementing a certificate revocation list is that it is a single point of failure and expensive to maintain. A CRL is comprised of public keys. The security administrator wants to increase the cipher strength of the company's internal root certificate. In this case, a CA would have to sign a stronger root certificate. An alternative to the CRL is the Online Certificate Status Protocol (OCSP). Use the OCSP to check the status of individual certificates.

Digital Certificates

The standard X.509 format is followed for certificates. It includes the certificate version, certificate holder's public key, serial number, certificate holder's distinguished name, certificate's validity period, unique name of certificate issuer, digital signature of issuer, and signature algorithm identifier

Certificate Specifics

Certificates can be issued for ecommerce, email, software, or device authentication. Setting up a PKI is the most secure way to log in to a VPN. Requiring client and server PKI certificates for all connections to the corporate Web site is the best mitigation against potential man-in-the-middle attacks. PKI would require the use of certificates to verify a user's identity. A secure company portal, accessible publicly but only to company employees, frequently fails to renew its certificates, resulting in expired certificate warnings for users. These warnings: Breed complacency among users for all certificate warnings and are irritating to the user but the traffic remains encrypted.

PKI

Public Key Infrastructure (PKI) encompasses the hardware, software, personnel, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

PKI allows two people to communicate securely without having to know each other prior to communicating. A public key Infrastructure is a pervasive system whose services are implemented and delivered using public key technologies that include Certificate Authorities (CA), digital certificates, non-repudiation, and key history management.

Recovery Agent

A recovery agent, typically an administrator, should be used if a user lost their private key. It allows a company to maintain access to encrypted resources when employee turnover is high. It stores information with a trusted agent to decrypt data at a later date, even if the user destroys the key

Key Escrow
Key escrow provides a system for recovering encrypted data even if the users lose private keys. It is the process of entrusting the keys to a third party.

Public Key
The public key is contained in the certificate and freely distributed. The recipient's public key is used by the sender to encrypt data. The public key of the root CA is found in a browser's trusted root CA list.

Private Key
The private key should be kept secret at all times. The private key in PKI It is used to encrypt the email hash in signed emails. A HSM is the most secure way of storing keys or digital certificates used for decryption/encryption of SSL sessions. Key compromise and CA compromise are reasons why a key may be revoked.

Public and Private Keys
In a standard PKI implementation the sender's private key is used to sign messages, wile the sender's public key is used to verify digital signatures, also note that the recipient's public key is used to encrypt messages, while the recipient's private key is used to decrypt messages. Use of public and private keys would allow each user to individually decrypt a message but allow anybody to encrypt it.

Registration Authority
Optionally, a registration authority (RA) will offload some of the work of a CA. The RA will do identity proofing on the registrant, collect fees, and give the registrant a passcode to retrieve their public/private key pair directly from the CA. Depending on the class of the certificate, all that might be needed is an email address. However, for Level 3, extended validation certificates the enrollee will have to present himself in person and go through a background check.

Trust Models
A single trust model is the easiest to implement, but not scalable or secure. A hierarchical trust model is the more scalable and secure model. In this model the root CA signs its own certificate and signs the certificates of subordinate CAs. The root CA is then taken offline so it cannot be hacked. The subordinate CAs issue certificates to users and devices. In a hierarchical trust the root certificate for the CA for a branch in a city was generated by the CA in a city in another country. PGP uses a peer-to-peer trust. This is also called a web of trust or mesh of trust. PGP can use a trust system where public keys are stored in an online directory.