Exam Manual

LearnSmart

CompTIA (SY0-201) Security+

By presenting complex topics as clearly and directly as possible, this LearnSmart exam manual intends to prepare candidates for CompTIA's Security+ (SY0-201) exam. Candidates who study this guide will become familiar with an array of security topics covered on the exam, including:

- Systems Security
- Network Infrastructure
- Access Control
- Cryptography
- And More!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

Security+ (SY0-201) LearnSmart Exam Manual

Product ID: 11886
Production Date: July 8, 2011

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

This Exam Manual will help you prepare for exam SY0-201, CompTIA Security+. Exam topics include: Systems Security, Network Infrastructure, Access Control, Assessments and Audits, Cryptography, and Organizational Security.

What to Know

CompTIA's Security+ certification is aimed at IT professionals who have two years on-the-job networking experience, with an emphasis on security. It is an entry-level, vendor-neutral certification. The Security+ certification a great stepping-stone to more advanced certifications, such as the ISC2 SSCP and CISSP, and the SANS GIAC. It also may be used in some Microsoft certification tracks.

This certification is well suited to network and security administrators independent of what industry they work in. The Security+ designation is achieved by passing one conventional format exam that covers topics such as communication security, infrastructure security, cryptography, access control, authentication, external attack, and operational and organization security. The Security+ certification demonstrates the candidate's knowledge of information security. It can help equip the candidate with the skills necessary to withstand hackers, and decrease costs associated with security breaches. Like other CompTIA offerings, once a person achieves the Security+, the certification will not expire.

Domain 1 - Systems Security

The full scope of system security concepts are an all-encompassing umbrella category of computer-related exposures, threats, risks and vulnerabilities. Any security issue corresponding to end-user applications and the underlying operating system falls under this categorical heading. Various types of threat, risk, vulnerability and exposure exist at the local level, where physical access is granted and authorization provided to perform computer operator tasks.

System Security Concepts

General system security concepts are governed by a few core standards and principles. These elements compose the foundation for larger system security constructs and establish the groundwork to build frameworks for robust security components.

System Security Standards

A system security standard forms the basis for exercising secure procedures and baseline for executing secure functions within the context of secure computing systems. System security standards are composed into formal security policies that dictate the overall practices and procedures governing an organization's operations.

- **Trusted Computer System Evaluation Criteria (TCSEC):** Also known as the 'orange book.' The TCSEC is an old standard that describes security levels operating systems. Security designations range from A to D, with D being the most secure. The C2 standard level was the goal which discretionary access control based operating systems like Windows, Netware, and Linux tried to attain. TCSEC was replaced by the Common Criteria.
- **Information Technology Security Evaluation Criteria (ITSEC):** A European security criteria based on TCSEC. However, ITSEC rates both functionality (with a rating of F for CIA), and assurance (with a rating of E). ITSEC was replaced by the Common Criteria.
- **Canadian Trusted Computer Product Evaluation Criteria (CTCPEC):** This is a computer security standard comparable to the American TCSEC ("Orange Book"), but somewhat more advanced. CTCPEC was replaced by the Common Criteria.
- **Common Criteria** (**CC**): The CC is an international standard (ISO 15408) for computer security. Its purpose is to allow users to specify their security requirements, to allow developers to specify the security attributes of their products, and to allow evaluators to determine if products actually meet their claims. It is considered the de facto security evaluation criteria that the international community follows.

System Security Threats

The practice and process of system security requires professionals and practitioners to maintain constant vigil over end-user interactions, application launches, system events and also keep abreast of current security topics. Only truly ambitious individuals will succeed in the dynamically evolving security realm, where one false move or absolute failure can sometimes unfairly overshadow a history of successful outcomes. Your entry into the security field begins with identifying local system threats, which is where most of the firefighting tasks happen.

Privilege Escalation

Multi-user computer systems are designed for interaction among numerous users and user groups, each having separate and incompatible permissions to perform various activities. For a system attacker, the ideal user account has administrative privileges on the system and is permitted to perform virtually any task—particularly those that further intrusion, infiltration or interception of valuable information. A *privilege escalation* attack exploits a configuration error, design flaw or exposed vulnerability in a privileged security application to gain illegitimate access to protected resources.

Virus

A computer *virus* is any form of malicious code that spreads from system to system by attaching itself to data or files. Viruses typically self-replicate on local systems, however they can extend to other computers by targeting network drive shares, removable media and other communal resources. Each virus is specifically designed to attack systems in a particular way and target particular areas. The following list briefly describes the different features and forms a virus may take:

- **Resident virus** – a terminate-and-stay resident virus permanently attaches to the host computer and operates in memory (RAM). It attempts to load before other mechanisms that attempt to analyze, detect and identify its purpose and origin and can bypass, interrupt or manipulate basic operating system functions.
- **Direct action virus** – an aggressive form that replicates and takes direct action when triggered by some condition, date or event. The direct action virus typically resides in system folders or the root directory path where it can be readily accessed and activated and carry out its tasks when the system boots up.
- **Overwrite virus** – a virus can partially or completely delete information contained in the files it infects, even replacing portions of application code with its own payload. Viruses of this kind are generally easy to identify with anti-virus software, as they generally tend to alter end-user and system applications in noticeable and identifiable ways.
- **Macro virus** – certain applications contain embedded scripting or "macro" languages enabling users to automate long series of operations as single shorthand actions. A *macro virus* targets these applications by containing code that replicates and replaces other macros to launch the virus payload when common functions are called.
- **Polymorphic virus** – a virus can avoid detection by through cyclic changes to its original form. Such a virus may encode or encrypt certain code segments that are transformed during runtime as usable code segments, then later encrypted differently than before to evade signature analysis and thwart behavioral analysis engines.
- **File infectors** – the traditional virus is a file infector that targets executables to cause direct or indirect execution of its payload. Most viruses fall under this category and are further classified depending on what is targeted and the actions taken during the infection process.
- **Companion virus** – another typical type of viral infector is the *companion virus*, one that accompanies another ordinary executable file. When the source file executes, control is passed to the companion virus and the end-user remains completely unaware.
- **Boot sector virus** – viruses may also infect the boot sector on a storage volume with its own payload to ensure that the virus always loads before the operating system. Though less common, these viruses still flourish since master boot records (MBR) and other disk allocation methods see continued use.

Worm

A *computer worm* is exploitive malicious code like a virus in that it self-replicates; however, all similarity ends there, as one thing a worm does (that a virus cannot do) is replicate directly across network media. Worms are also generally designed to leverage some software, system or service vulnerability to enable propagation across network connections.

Trojan

The classic Trojan horse is a class of computer threat that apparently perform some desirable function (launch a game, activate an e-card) but instead transparently or invisibly conducts malicious activity to allow unauthorized access and/or usage of the affected machine. A Trojan horse application is often disguised as a legitimate application or portion of some software suite and opens a back door into the system when invoked by the user unless designed to trigger upon some condition, date or event.

Spyware

Computer software installed surreptitiously and without the owner's or operator's consent and then attempts to harvest personal information (e.g., usage trends, software licenses, sites visited), invades privacy or manipulates browser activity is called *spyware*. Such software appears to be legitimate but contains hidden functionality that is otherwise undesirable and unwarranted.

Spam

Unsolicited bulk email messages (particularly those sent indiscriminately to tens, hundreds or thousands of subscribers) is called *spam*. Spam is the electronic form of postal "junk mail", filling inboxes with useless and unrequested material typically used for marketing purposes. Spam can be malicious, but mostly it takes the form of dubious advertisements or money schemes.

Adware

Advertising-supported software or *adware* is any program that automatically displays or downloads advertisements during application usage. Adware may accompany or integrate into a larger software package and install usage monitoring components, but mostly its purpose is to custom tailor advertisements for targeted users.

Certain types of adware are also spyware if they perform the same information gathering and snooping functions. However, adware is mostly harmless in that it only produces advertisements for goods and services or extended features not included as part of some free or limited software package.

Rootkits

Malware consisting of a program or collection of programs designed to hide one's presence and activity on a compromised system is called a *rootkit*. An attacker must first gain access for the rootkit to be truly effective and various layers of the operating system are manipulated to disguise activities, applications and connectivity from watchful administrators.

Botnets

A collection of compromised computers operating in a collected, cohesive fashion (coordinated by a controller computer) is called a *botnet*. Individual computers are captured and controlled by a *bot* or malicious application that leverages remote control for an attacker, the *bot herder*. Command and control channels are often basic IRC channels containing other bots within the botnet.

Logic Bomb

Any malicious code that lies dormant until triggered by some condition, date or event is called a logic bomb. A trusted insider could emplace a logic bomb to cause damage in the event of their firing or as part of industrial espionage for a competitor. Generally, logic bombs appear as part of some other unsuspecting software package and are invoked without the end-user's knowledge.

Hardware and Peripheral Security Risks

Computer security threats, risks and vulnerabilities are not restricted to software; even hardware can cause significant security violations. Several key aspects of the system require adequate protection against tampering and manipulation by unauthorized parties. Sensitive applications, services and processes can be disrupted and security mechanisms bypassed by employing or modifying various hardware configurations.

Basic Input/Output System (BIOS)

Every PC has a BIOS, which is specialized boot firmware designed to identify and initialize system devices prior to turning over control to the operating system. A computer's BIOS prepares the machine in a process called *bootstrapping* or just *booting*. Most computers provide basic access to BIOS settings through configuration menus invoked prior to boot-up. When users can perform unauthorized changes to BIOS settings they can bypass local security settings and violate company security policy.

The most common approach to securing the BIOS includes setting an administrative password so that users cannot change boot device priorities, enabled or disable features or utilize unauthorized devices. If an attacker can boot from external media, none of the system's local security settings are effective and the internal storage volumes themselves are completely open to attack (installing backdoors, Trojans or rootkits) and manipulation (data theft, tampering or trashing).

USB Devices

Any removable storage media can present a series of issues in the protected workplace. Sensitive information can be passed beyond security controls and taken outside of the security perimeter. An individual can also knowingly or unknowingly introduce malware to the local system or attached network or use bootable USB media to bypass local security restrictions. Specialized USB devices can also harvest information, interrupt operation or copy data on-the-fly and in some cases transparently to the end-user.

USB devices access should be selectively enabled and tightly controlled to prevent users from bypassing restrictions, overcoming security or subverting control. Malware infections make little distinction about their storage media, just so long as it holds (and in some cases transports) its code for future use. Sensitive data cannot determine what storage devices are authorized or unauthorized, and will gladly store wherever accepted.

Mobile Phones

The emergence of the mobile phone marked a trend that would soon find itself merging with other portable technologies (e.g., image capturers, video recorders, music players, digital organizers) and converging on the corporate workspace. Because mobile phones are no longer mobile phones, they pose a considerable security threat for a number of reasons.

Bluetooth and 802.11 wireless have become a popular item among recent cell phone designs, which means that attacks can originate from or be destined for equipped phones. Newer phones are also capable of executing a range of compiled and scripted code, leaving many forms of computer-related attack feasible on these platforms. Phones equipped with cameras are capable of photographing sensitive equipment and information that is otherwise restricted to authorized parties.

Removable Storage

All removable storage does is create a temporary attachment point for users to access and copy data or execute files. Like USB (and Firewire) devices, removable storage media often helps end-users bypass local security restrictions that affect other portions of the system. Users may bypass safe storage requirements when operating in highly sensitive areas, relocate and expose sensitive data beyond the security perimeter, and introduce unsafe code or executable data into protected environments.

Network Attached Storage (NAS)

A common arrangement for larger networks is to place storage volumes in full view of the entire network scope so that all users may centrally access them. NAS devices create an attachment point between storage volume and network media thereby giving access to devices that are typically enslaved to a single computer.

Without proper permissions, unauthorized users may deliberately access confidential files and sensitive data. Left unchecked, malware can also easily propagate to end-user workstations and back-room servers via NAS drives. NAS security centers around administratively-configured group and individual Access Control Lists (ACLs) with restrictive access virtually segregated (VLAN and router rules) and physically separated.

System Hardening Practices

The practice of hardening a computer system follows a series of protocols, procedures and policies that define and describe system security. Blocking unused ports, removing unnecessary services, deleting unused applications and plugging all known holes are just some activities involved in the system hardening process.

Hotfixes, Patches and Updates

The term *hotfix* originally described remedying code fragments (called *patches* or *updates*) to currently-running applications but has now become to mean a single, cumulative package that includes files that resolve an identified problem in some software product. In some instances, a hotfix may resolve only a customer-specific issue and not reach widespread distribution channels.

Microsoft Windows uses the term *service pack* to describe collections of fixes, enhancements and updates for various related products. They can also be incremental in that a later service pack contains files not present in earlier service packs or cumulative in that it contains all previous files.

Patch Management

The release cycle for fixes, enhancements and updates follows no set schedule. Depending on severity and necessity, a hotfix or service pack may be released instantly upon vendor notification or follow a lengthy prioritized development cycle for later release date.

Patch management is the practice of routine maintenance and upkeep of application, service and system patches. It's an area of systems management driven by a cycle of acquiring, validating and implementing patches to computer systems in a methodical manner and requires up-to-date knowledge of current security issues and trends.

Group Policies

Centralized configuration and management of multiple computers and remote users in a networked Active Directory environment are controlled through *group policies*. Entire collections of end-user application, desktop, service and environment settings can be applied individually or collectively via group policy along with administratively-defined security attributes.

Organizations utilize group policy to retain control and restrict certain actions that might pose security risks, such as blocking access to unauthorized sites or prohibiting downloaded files from installation.

Security Templates

A security template defines the secure basis for building ... or creating ... Security templates simplify the process of managing large computer environments and streamline the implementation of several interrelated devices. Windows Server uses predefined security templates to increase network security, which can then be modified to suit site-specific requirements. Similarly, Linux systems using policy enforcement systems can also create, modify and utilize security templates to achieve a secure baseline.

Configuration Baselines

A *configuration baseline* is a configuration management strategy that establishes all basic principles and best practices. Configuration baselines are used as the basis for future builds, releases and changes of system software and hardware components within a hierarchical computing environment. Baselines are ideal for establishing a default secure disposition for various computer and network elements using security templates across several devices.

Application Security

The realm of application security has become a hotbed of activity. Attackers have found higher success rates and lower risk factors in attacking weak applications rather than weak platforms (such as challenging operating systems or network stacks). Web clients, servers and scripting provide plenty of opportunity for rapid development that cuts both ways—sometimes in favor of the attacker.

ActiveX

Microsoft developed the ActiveX component object model (COM) for creating specialized software components used to build feature sets and encapsulate reusable functionality. ActiveX controls are small program building blocks used to create distributed applications that work over the Internet through Web browsers. Developers can create customized applications for gathering data, viewing files and displaying animated content.

ActiveX security relies solely upon end-user discretion and judgment. ActiveX controls are digitally signed to prevent unauthorized alterations via "authenticode" and certified by a trusted Certificate Authority (CA). However, ActiveX components are behaviorally unrestricted and users must selectively choose to authorize programs. Malware has been written in ActiveX to prove its effectiveness as a platform for attack, so always block unsigned controls.

Java and JavaScript

Java and JavaScript share a similar security model. Downloaded scripts are executed within a restricted sandbox environment to shield the operating system from the unintentional or unforeseen consequence of running untrusted or unverified code. Scripts are generally permitted access only to data relevant to the current document but no access is granted to the local file system, memory space of other programs or the operating system's network stack.

Containment of unverified code prevents malfunctioning or malicious code from rendering damage to the user's working applications and environment or the operating system's processes and services. For all intents and purposes, Java and JavaScript applets are all considered hostile and treated with equal distrust and only make exceptions for code that originates from trusted sources.

Browser Issues

The Web browser connects clients to the Internet's vast array of pages and portals. Part of the problem with the openness of Internet connectivity the fragile trust model between two entities. Since few parties are able to make in-person verifications about the other entity, we rely on credentials and certificates signed and verified by trusted third parties.

Because of their widespread usage and versatility, browsers are susceptible to all sorts of hijacking attempts, invalid code execution, unauthorized information gathering, personal information harvesting and fraudulent redirections. Blocking unsigned controls and visiting only trusted sites isn't enough: malware can redirect your system to an untrusted site that presents itself as a trusted party.

Buffer Overflows

A buffer overflow attack redirects program execution flow to perform attacker-defined tasks by overfilling the boundaries of a stack or memory-based storage region. By carefully crafting a payload and trampling over important code constructs, attackers may leverage control over a program that would otherwise crash or corrupt data. Buffer overflow attacks may target applications, services and operating system (kernel) code.

Cookies

Internet cookies are text files that help track and maintain various site-related activity from your Web browser. Cookies facilitate authentication, session tracking and maintenance of user-specific data (such as browsing preferences). They are simply non-executable pieces of data that affect the operation of a web server—not the web browser—in very specific ways, but are generally viewed as untrustworthy because cookies keep tabs on browsing and viewing habits.

Open Mail Relay

An open mail relay is any SMTP server permissively configured to allow any unauthorized source from the Internet to pass email, particularly that destined to or originating from unknown users. Default mail servers left security as an administrative afterthought and made no distinction or discretion about what email was passed—the server is just doing its job. However, open relays have led to extensive email spam attacks that have overwhelmed victims and unwitting participants alike.

Instant Messaging (IM)

The instant messaging platform is both beneficial and detrimental to the corporate network, depending upon its application. While developers may correspond through IMs during the development process, data entry users may be socializing outside of work-related channels and topics. Furthermore, an IM application is often itself a potential target and vector for attacking into the network.

Confidential communications may be eavesdropped upon or sensitive data intercepted that is otherwise assumed safe. Some IM applications provide internal file transfer and remote connection features that enable users to bypass network perimeter restrictions or content accessibility policies.

Input Validation

An application that sanitizes the data received from users, files or other programs and services is said to provide *input validation*. Cleansing input of unsanitary constructs or illegal sequences purifies the input stream from tainted values that can alter program execution.

Web applications commonly receive lots of invalid inputs from various unchecked sources—not all of which is malicious—but particularly clever coders can manipulate an application's flow to reveal sensitive information, store malicious code, apply configuration changes or other forms of attack. Input validation attempts to cripple such attacks by removing any unnecessary elements.

Cross-Site Scripting (XSS)

An increasingly popular form of attack targets vulnerabilities typically found in dynamically-generated Web page content enabling malicious users to inject code or data into the pages of unsuspecting victims is *cross-site scripting* (XSS to differentiate from cascading style sheets). An exploitable vulnerability can leverage control or bypass security restrictions to provide a platform for further attack—such as phishing or browser exploits.

Redirection and misdirection are a major component of XSS attacks. XSS can be used to hijack an active Web session, snoop on private postings, guide unwitting users to attacker-controlled servers and perform other types of attack.

Security Applications

Defending against the various forms of network and system attack requires several concentric rings of security. A defense-in-depth strategy is possible through several layers of protective software, each of which is designed to concentrate on a few core set of issues.

Host-Based Intrusion Detection System (HIDS)

An intrusion detection system (IDS) generically defines a class of security software that identifies sources of attack and intrusion either by observing behavioral anomalies against a secure baseline or recognizing patterns in application or network data. A host-based IDS (HIDS) works with respect to the local system, where all local activities occur in full view of the security application.

HIDS analyzes and monitors internal system interactions and observe the operating state of the computer at all times. When an anomaly or attack is suspected, the system raises alert with administration to prompt a response.

Network Firewalls

The primary purpose of a *network firewall* is to logically segregate public and private networks, but firewalls may also separate internal subnetworks within a larger network scope. Firewalls provide private networks basic protection against sources of public attack and enable administrators to apply ACLs and security policies to network traffic. As such, a firewall is the first line of defense in any network and provides a central choke point for externally-bound internal connections. When a firewall has two or more separate network segments passing traffic to different IP addresses it is called *multi-homed*. An optional third port may provide a DMZ for public access to company servers.

Common types of firewalls include:

- **Application-level proxy:** resides at OSI layer 7 (Application) to provide a single proxy to provide strict control over for high-level protocol connections.
- **Circuit-level proxy:** resides at OSI layer 3 (Network) to review header information before determining access, which is applicable to multiple protocols with high-level control.
- **Packet filtering:** resides at OSI layer 3 (Network) to scrutinize protocol address, port and parameters before granting or denying access.
- **Stateful filtering:** advanced packet filtering that maintains connection state (startups and teardowns) to identify invalid traffic patterns while applying administrative rules.

Anti-Virus Scanners

Personal and corporate antivirus scanners have become a mainstay of the security landscape. Antivirus scanning seeks to identify, isolate and incise viral infections and other malware from affected systems. Traditional antirivus scanners narrowly focus on viruses, but modern software suites have adapted to analyzing, neutralizing and eliminating a range of malware that includes bots, rootkits, Trojans and worms.

There are different methods for identifying viruses and malware that include:

- **Signature-based detection:** the most common method of identifying malware by checking patterns in software against dictionaries of known malware "signatures".
- **Behavioral-based detection:** malware tends to behave in certain identifiable ways, so behavioral analysis can flag suspicious binary behavior and prompt the user for action.
- **Heuristics-based detection:** sophisticated antivirus software identifies new forms of malware through file analysis and file emulation.

Anti-Spam Filters

Email-driven spam is a dynamic problem of exponential proportion because of the free accessibility and cost of sending electronic messages. The problem has now spanned other technological divides to include phone-based text message spamming and Voice over IP (VoIP) systems. Anti-spam techniques attempt to detect spam using a variety of methods including DNS blacklists, country or network block filtering, spamtrap bogus email addresses, RFC standards enforcement and a variety of other means.

Virtualization Technology and Security

The purpose and application of virtualization technology is to provide a method of logically rationing physical resources to create multiple virtual computing contexts. Virtualization maximizes resource utilization and provides the most efficient use of singular system hardware resources. It also provides a more comprehensive means for centrally managing and maintaining multiple virtual computing environments and enhanced redundancy for enterprise physical computing environments.

Virtualization technology also enhances security by isolating the underlying operating system from all of its virtual counterparts. All activity is contained within the confines of the virtual computing environment, except for rare cases where an attack escape or transcend that boundary.

Domain 2 - Network Infrastructure

Every network is architecturally defined by its applications, connections, equipment, interfaces, protocols, standards, services and topologies. The network infrastructure is a complex landscape involving many interrelated components, each of which has its own set of security concerns and considerations. As a security practitioner, you must be knowledgeable in the basic elements that comprise the network infrastructure and educated in the means and measures of protection.

Basic Network Threats

A basic network threat is one that is common, known and well-understood. Certain types of attacks are frequently repeated and (usually) easily defended but persist anyway. The network environment will encounter an attack from all angles and all sides from a variety of sophisticated and unsophisticated attackers (and attack methods). Security+ certification examines your ability to identify and handle a number of typical security incidents affecting the network and its interrelated parts.

Antiquated Protocols

As organizations grow and accumulate various software applications and protocols to accomplish various business functions some of those elements reach *antiquity* or obsolescence. Once a protocol is antiquated (in computer terms) it's deemed unfit for consumption, particularly where it poses a negative security impact and has a more suitable replacement. Early communications protocols often lacked proper security features to prevent eavesdropping, hijacking, interception and other forms of attack.

Perhaps the biggest problem with relying on antiquated protocols is that their threats and vulnerabilities aren't always easily identifiable or readily known. New employees may be left uneducated and unaware of these protocols, which further complicates the matter. Antiquated protocols should be identified, evaluated and replaced with strong alternatives where applicable.

TCP/IP Hijacking

Client-server connection or *TCP/IP hijacking* involves an attacker forcibly gaining control over a legitimate conversation between a trusted two-party connection. Session hijacking is possible when the attacker is able to intercept transmission details between the two sources (being positioned somewhere along the line between source and destination) and use them to impersonate the legitimate client connection.

Null Sessions

Null session attacks target unprotected Windows interprocess communication (IPC) shares and provides unauthorized remote access. Older Windows products have insecure default settings that enable null session access (non-login interactivity) but newer versions (Windows XP and better) have corrected this issue.

An attacker attempts null session access to enumerate properties on the remote target, which is prelude to an attack. The attacker maps out the remote host by identifying the user accounts and remote shares, then uses this information to stage an attack.

Spoofing Attacks

A *spoofing attack* is another form of abuse on identity and trust. Spoofing appears in many forms as an attempt to gain authorized access by an illegitimate party posing as a legitimate source. An assumed identity links the various forms of attack: sending email under a false identity, manipulating target network stacks using bogus protocol information, and forging parameters in a chain of messages or communication are just some examples.

Man in the Middle (MitM)

An attacker is emplaced between a trusted client-server connection can perform subtle *man-in-the-middle* (MitM) manipulations, which is the interception and tampering of data by an unauthorized third party. Email, FTP, Web and even Secure Shell (SSH) connections can be subject to MitM attacks. MitM involve the interception and entering into a private conversation and subsequent eavesdropping or modification of data in a trusted chain of communication.

TCP Replay

A TCP replay attack reuses captured network packets in modified form against an original party of some trusted network conversation. Weak network stack implementations may foolishly parse and process the tampered protocol data and establish a trusted but bogus connection. The TCP relay attack may be prelude to further attack, such as activating an authentication mechanism that in turn enables a secure connection from an attacker-controlled (thus unauthorized) source.

Denial of Service (DoS)

As the name implies, a denial of service attack renders legitimate resources unavailable to authorize entities (e.g., applications, users, services). DoS attack frequency and intensity varies: it may require a single packet or a sustained flood of service requests to saturate a server or service from responding in a timely fashion. Local DoS attacks render individual workstation or server computers unresponsive while a remote or network-specific DoS affects multiple users and connections.

Distributed Denial of Service (DDoS)

The scalable version of DoS is the distributed denial of service or DDoS attack. Multiple computers employ the same application, platform and protocol attack methods as the DoS variety but with the magnified impact of tens, hundreds or thousands of participants. Harnessing large groups of zombie computers—attacker-controlled client PCs and sometimes server computers—leverages the multiplying power of several workhorses to saturate and overfill a target so that legitimate users are denied access.

DNS Kiting

Kiting is a term originally used to describe various forms of check fraud that takes advantage of the time between check negotiation and clearance at the account holder's bank. Similarly, *DNS kiting* exploits the domain name registration grace period where persons or entities register, cancel and re-register the same domain within that grace period to avoid paying registration fees. DNS registrars often permit a 5 day grace period as part of the registration and cancellation process and triggers a refund when done within this window of time.

DNS Cache Poisoning

The Domain Name Service (DNS) is basically a caching service that maps information related to assigned numeric IP addresses and easily-memorable domain name identifiers. DNS translates between the dotted-decimal notation addresses (63.146.189.101) and the domain name (preplogic.com). DNS cache poisoning occurs when a server receives information that does not originate from an authoritative source (and is therefore illegitimate and invalid) and serves it to unsuspecting victims. Subscribers of an ISP are affected when their DNS lookups produce incorrect results (i.e., redirection to a bogus or imposter site of the attacker's choosing).

Address Resolution Protocol (ARP) Poisoning

ARP spoofing or *ARP cache poisoning* is an attack against Ethernet that enables an attacker to sniff frames on a switched network and redirect endpoint traffic through an attacker-controlled machine. It operates on the principle that faked ARP messages can be sent with sufficient volume and regularity that false associations between hardware (MAC) and protocol (IP) are possible, thus invalidating the ARP cache.

An attacker may also launch DoS or perform man-in-the-middle (MitM) attacks through a well-placed machine under control. ARP is not designed for ID validation on its transactions, which makes this attack feasible on modern networks that do not protect the ARP cache or maintain static route tables.

Network Design Components and Elements

Any given network infrastructure is comprised of many commonly recurring components. Familiarity with these components, functional roles and operational traits, and respective attack and defense strategies is essential to your job as a security professional.

Switches

Network *switches* are OSI protocol layer 2 (and sometimes layer 3) devices that connect separate computers and network segments. Switches come in all shapes and sizes from compact four-port Ethernet units to enterprise-class 48-port Gigabit Ethernet designs. Since switches forward frames based on MAC address, network traffic is delivered directly between sender and recipient (unlike hubs, which broadcast all traffic on all ports). Network switches are also capable of supporting VLAN creation to enhance corporate network administration and security.

Routers

Network *routers* are switching devices with enhanced traffic handling capabilities. While switches are used primarily to join local network segments, routers establish connectivity between public and private networks (or among separate private networks). A router communicates in network-layer (OSI layer 3) protocol packets and multi-protocol routers translate between several different network protocols. Routers forward packets based on source and destination addresses and may provide basic security through ACLs.

Demilitarized Zone (DMZ)

A network's *demilitarized zone* (DMZ) is the dividing line between a public and private network. In most arrangements, the DMZ establishes a physically separate buffer and containment area for public-facing private company servers. This portion of the network is kept separate from the protected internal network, providing a compromise between offering public services and operating private servers without fully exposing private networks to high risk or hostile environments.

Virtual LAN (VLAN)

The Virtual Local Area Network (VLAN) is a logical network arrangement that permits two physically separate networks to operate as if locally attached. Actual LAN segments that comprise the VLAN may be spread across a campus, city or different regions or territories throughout the country. A single organization may employ several individually-protected VLAN broadcast domains (i.e.., Human Resources and Data Entry departments) to isolate cross-contaminations (such as virus and worm outbreaks), separately manage departmental groups, and so forth.

Network Address Translation (NAT)

An organization may share a single external (Internet) connection among several internal computers using *network address translation*, which is a one-to-many mapping of public-to-private IP address spaces. NAT reduces the need for several public IP addresses through and ISP by establishing an administratively-defined address pool mapping the internal network and repackaging those connections as a single source (usually centralized at a gateway or router device) without exposing those internal endpoints to the Internet.

Network Access Control (NAC)

Network access control is a computer networking security strategy and solution that attempts to unify endpoint security technology (e.g., antivirus, HIPS, vulnerability assessments) through a set of protocols to define and implement security policies describing network access. NAC also defines user or system authentication and network security enforcement procedures. A significant usage of NAC is to enforce system health requirements that are checked upon accessing the network: systems deemed "unhealthy" (outdated signatures or software) are administratively prohibited to connect.

Subnetting

A subnetwork or subnet is a compartmental collection of designated IP addresses that correspond to end-user computers, gateway devices, company servers and other intermediary devices and network endpoints. *Subnetting* is the process of logically dividing a network into classes of smaller networks to prevent Ethernet collisions and address assignment conflicts.

Subdivided networks can be individually guarded by firewalls and granted different access rights and network permissions according to job functions. Common classes include Class A, Class B and Class C subnets that all correspond to increasingly smaller sizes of network segment.

Telephony

Telecommunications or *telephony* encompasses the general use of phone equipment to provide voice communications over great distances. Telephony involves the transmission and translation of analog voice information to digital voice formats to provide long-haul connections for human communication.

As a catchall terminology, telephony refers including digital computers, wireless phones and voicemail systems. Each of these categories provides plenty of security risk, threat and vulnerability for an organization that seeks to preserve confidentiality and protect privacy.

Network Security Tools

All aspects of network security operate in concentric rings of overlapping protection. At the network level routers filter basic traffic patterns, switches partition VLAN segments, intrusion detection systems identify and intercept protocol attacks.

Network Intrusion Detection System (NIDS)

Certain network attack sequences leave traceable patterns that become scanning engine "signatures" used to detect further occurrences of attack. A *network intrusion detection system* identifies malicious network activity by matching signatures against observed traffic and alerts administrators to threatening or risky conditions. NIDS observes for indications of DoS attacks, port scans, invalid connection requests and malware behavior.

Network Intrusion Prevention System (NIPS)

A *network intrusion prevention system* performs the same duties as NIDS but with a more active role: instead of alerting administrators (like NIDS) the NIPS takes immediate action. Upon detection of a certain attack or suspicious traffic pattern the NIPS will take some predefined action against the event—such as closing the connection, issuing firewall block rules against the host, and so forth.

Network Firewalls

The *network firewall* is a first line defense mechanism for safeguarding corporate networks from the unruly and untrustworthy Internet. To simplify, the firewall is a software system or group of systems designed to enforce and manage network access policies. A firewall may be hardware-accelerated in that it operates from a specialized hardware platform or offloading network appliance, but all of them apply filtering rules against traffic moving into (ingress) and out of (egress) a network.

Firewalls help segregate subnetworks into separately-protected entities and can create demilitarized zones (DMZs) for public access to private servers without exposing internal endpoints. Using a firewall is instrumental to securing the network against most basic forms of abuse and attack but cannot adequately protect against legitimate traffic bearing illegitimate code.

Proxy Servers

A *proxy server* services requests by playing a middleman role, brokering deals between client and server. By nature, the proxy evaluates connection requests against administrative rules and may selectively filter traffic matching certain criteria or conditions. Proxies keep internal machines hidden and anonymous and enhance network performance by caching commonly-requested resources. Proxy placement may be at individual workstations or centralized at a gateway server.

Honeypots and Honeynets

Network *honeypots* are fake servers setup as low-hanging fruit to entice attackers away from sensitive systems and as containment for observing intruder or automaton (i.e., bots and worms) behavior. An organization uses honeypots to draw unwanted attention away from real computers and operators and serve as early-warning indicators of a break-in. A network composed of honeypots is called a *honeynet,* which is used to monitor more diverse network conditions and interactions among more sophisticated attackers or attack strategies.

Internet Content Filters

An *Internet content filter* constrains various types of information that is permitted across the network, like applying ACLs to application-layer traffic. Keywords, hostnames and content descriptors are just a few criteria the general class of content filters will screen for to groom traffic of unsavory material. As there are no restrictions on what is permitted on the Internet, individuals and organizations are able to control and restrict content delivery to end-users especially where material is of objectionable or questionable nature.

Network Protocol Analyzers

Computer networks are monitored using *network protocol analyzers* or Ethernet "sniffers". Such devices are capable of capturing, filtering and displaying network traffic so that administrators can visualize various interactions and interconnections. The sniffer is a powerful protocol visualization tool that is also capable of decoding protocol payloads, enabling observers to dissect and study higher-level communications—including instant messaging, file transfers and email messages.

Access and installation of protocol analyzers should be administratively prohibited by all but a select few personnel. Guarding against unauthorized analysis is made possible by employing encrypted communications protocols and services or wrapping plaintext protocols in cryptographic tunnels.

Network Device Vulnerabilities and Mitigations

Network perimeter devices are most closely positioned to sources of attack. They define the outer edge of a corporate network and create an invisible barrier that encapsulates the internal network. Attackers must first pierce through an arrangement of front-line defenses and devices, bypass content and policy filtering mechanisms and leapfrog internal devices to reach protected endpoints. As a security practitioner, you must learn to create a defense-in-depth strategy capable of containing multiple attacks even while sustaining secondary and tertiary breaches or failures.

Privilege Escalation

Weakly-passworded network appliances, gateway hosts and routing devices are susceptible to privilege escalation attacks. Broken configurations and vulnerable software also create the potential for such attack, and an intruder with control over intermediary network devices can observe private conversations and connections among multiple parties. Now instead of attacking a single system, the intruder can command control over several different systems in a collective manner.

Network devices should follow the same maintenance (i.e., update and upgrade) routines and given an appropriate level of security treatment. Enforce strong password policies across all routing devices, network appliances and intermediaries, update software components particularly as security issues arise and adhere to a well-developed network security policy.

Weak Passwords

An attacker's job is trivialized wherever user accounts utilize weak passwords. Poorly chosen passwords using easily-guessed or predictable information (e.g., dates, names, events, hobbies, interests) can be determined manually and mechanically. Dictionary entries, proper names and family pets are terrible choices; shortened phrases, mixed capitalization and numeric addition or substitution provide much stronger password choices.

Enforce strong group and network policies demanding password expiration periods; check against easily-guessed, common or reused passwords; and set length and difficulty specifications for assigning new passwords.

Backdoors

A *backdoor* is any unauthorized, unguarded and undocumented manner of access that bypasses normal security protocols, processes and procedures. Planted backdoors are a secretive, underhanded way of securing reentry into a protected environment and enables attackers to intrude upon systems through unconventional and undetected channels. Certain types of backdoor (such as rootkits) contain programs that further aide in concealment once an attacker gains entry into a safeguarded system.

Default Accounts

Next to weak passwords, *default accounts* are among the top two most popular "easy entry" passes into protected systems and networks. Vendors often implement default accounts in popular software products for end-user convenience. Many end-users don't change these defaults and attackers are keenly aware of default account access and know when they stumble upon an easy target. Change default account names and passwords for any product (i.e. wireless router, operating system) and disable those not in use (i.e., guest account).

Denial of Service (DoS)

As the name implies, a denial of service attack renders legitimate resources unavailable to authorize entities (e.g., applications, users, services). DoS attack frequency and intensity varies: it may require a single packet or a sustained flood of service requests to saturate a server or service from responding in a timely fashion. Local DoS attacks render individual workstation or server computers unresponsive while a remote or network-specific DoS affects multiple users and connections.

Wired Media Vulnerabilities and Mitigations

Differing wired technologies suffer from different types of weakness and vulnerability, but all forms are susceptible to attack—including fiber optics. Attack strategy, sophistication and severity varies by tactic, technique and technology. Security+ certified practitioners are versed in a number of common attacks against wired and wireless vulnerabilities.

Ethernet Security

Several arising issues affect Ethernet security. Ethernet is a broadcast system: messages sent by any computer can potentially be observed or modified by an unseen third party. Even switched networks can be tricked into redirecting packets via protocol forgery and cache poisoning.Peer networks, network file systems and multi-user file sharing services are common aspects among Ethernet networks and present opportunities for attack.

Since most Ethernet protocols were designed without security in mind, many are implemented in plain-text protocols that reveal significant amounts of private information to unseen observers—which has given rise to encryption popularity. Lastly, packet forging or attacks against trust and identity are well-established and must be handled accordingly and appropriately.

Vampire Taps

The so-called *vampire tap* physically connects a station (e.g., computer, printer) to a coaxial cable network by clamping directly onto the wire and piercing a spike into the inner conductor. Spikes on the vampire tap clamp into the outer conductor and an *attachment unit interface* (AUI) joins endpoint device and network tap. Vampire taps permit arbitrary connections to be made on existing physical cable connections while currently in-use, enabling administrative expansion without interruption.

Wireless Media Vulnerabilities and Mitigations

The nature of wireless communications doesn't make it more or less secure than wired media: it's equally insecure. Taking over a wireless AP yields similar results to hijacking a router or gateway server: a harness of control over multiple ongoing network conversations.

Data Emanation

Data emanation is the unintentional disclosure of information through acoustical, magnetic or radio frequency energy. Certain electronic computing devices radiate sufficient emission strength that passive observation is possible even at a distance. Display terminal screen content can be reconstructed from RF emissions, shielded and unshielded RS-232 data can be recorded and reconstructed several meters away and most recently typed keyboard entries—even on "quiet" keyboards—can be recorded and reconstructed using a generic microphone. Most importantly, wireless radio signal coverage often oversteps the boundaries of the company building or campus. Radio signal propagation outside these boundaries can create data emanation potentially revealing useful information for network attack.

Wardriving and Wireless Broadcast

Freely broadcast wireless transmissions suffer from a similar problem as data emanation. The practice of actively seeking wireless radio devices and mapping network entities from a moving vehicle is called *wardriving*. Laptops and PDAs are most commonly used, but specialized designs comprising multiple antenna arrays and adapter cards are also used. GPS may also be employed as a means to measure and mark locations for an overhead visualization of wireless hotspots.

Wireless networking uses Service Set Identifiers (SSIDs) to identify 802.11 LAN segments and the most direct means by which wireless networks are discovered. Disabling SSID broadcast alone is insufficient to prevent discovery through wardriving or other practices. Use VPNs to foil eavesdropping, isolate APs from the internal network, eradicate rogue APs, filter unauthorized MACs and confine radio coverage to internal assets.

Bluejacking and Bluesnarfing

Bluetooth (BT) wireless communications are not invulnerable to attack. As a simplistic wireless protocol it provides weak security against casual and complicated techniques alike. *Bluejacking* is a method of issuing unsolicited anonymous text messages to BT-enabled mobile phones. *Bluesnarfing* is unauthorized access (and copy) of information using a BT wireless connection. Sophisticated attacks can coerce passing BT-enabled phones to dial attacker-controlled long distance numbers and rack up calling charges of unsuspecting subscribers.

Rogue Access Points (APs)

There are many problems with *rogue APs*, which are basically unauthorized wireless installations on a protected network. A rogue AP exposes unsuspecting clients to all sorts of attack (e.g., hijacking, phishing, data theft) and backdoor provide access to unauthorized parties. It can also destabilize a wireless network by causing conflict and confusion among connecting client devices and cause other disruptive harm. Detection of rogue APs is possible through wireless intrusion detection systems and radio spectrum monitoring for unauthorized entries.

Weak Encryption

Cryptography is the practice and study if hiding information through encryption; *cryptanalysis* is the science of analyzing and deciphering codes, ciphers and cryptograms. Algorithm and key strength are instrumental in defending against cryptanalysis and "code breaking" attempts. Weak encryption algorithms (and weak encryption keys) compromise the integrity and strength of a cryptographic implementation and eliminate all confidence in privacy. A weak algorithm or weak implementation is one proven broken and insufficient to defend against probable attack and creates weak links in much a larger security chain.

Domain 3 - Access Control

Every multiple-user computer system utilizes login accounts to distinguish individual account holders and assign varying permissions based upon end-user job roles and responsibilities. *Access control* is the encompassing practice of allowing and denying access, entry or usage to some protected resource by authorized and unauthorized individuals or groups.

Access control methodologies are the pervasive protocols and procedures that establish secure baselines and practices. Access control mechanisms manage both physical (i.e., entry to server rooms) and virtual resources (i.e., entry into server computers). Enforcement of access control methodologies through access control mechanisms entails the following:

- Measures taken to grant or deny access to resources for entities (users, computers, services) that have been successfully authenticated.
- It is being able to access necessary resources, and then being able to control those resources.
- To understand access control, make sure you know the differences between authentication, controlling access, authorization, and accountability.

Access Control Best Practices

All best practices are derived from a tried-and-true activity, method or process for achieving some task while delivering a particular outcome or near-optimal results. Access control best practices draw upon decades of computer security experience and formulate a common basis for analyzing, implementing and managing computer security systems.

Implicit denial

An *implicit deny* security stance views all things as suspicious that aren't specifically and selectively deemed permissible. An open network computing environment where anyone or anything may connect implicitly allows traffic, whereas a safeguarded network boundary that only permits certain IP addresses and/or service ports and blocks everything else implicitly denies traffic. Traffic that is blocked to certain ports or from specific addresses is said to *explicitly* deny.

Principle of least privilege
The *principle of least privilege* is an important security concept and design consideration that grants the lowest amount of privilege possible to perform some task. Access rights are assigned according to what an individual's roles require such as opening some file, modifying some data and viewing some results. In a security context, this restrictive permission protects against giving users sufficient rights to damage or disrupt sensitive higher-level functions and processes.

Need to know
The *need to know* principle dictates that employees should only be granted sufficient information to perform designated tasks—and nothing more. Conceptually speaking, this policy principle complements the principle of least privilege and helps achieve similar security objectives by reducing the amount of damage caused by any individual leaving the company or manipulating the company. Without formal information classification and security labeling practices, the need to know sensitive or privileged is the strongest preventive practice against tactics.

Separation of duties
A *separation of duties* selectively assigns access rights focal to a person's requirements to complete a given task. Separation of duties creates an appropriate level of checks and balances upon the activities of individuals operating in a given job capacity by preventing any one individual from gaining too much insight or control over business operations. In a security context, separation of duties disseminates the tasks of a particularly sensitive job among multiple users who function in individual capacities rather than as a collective group effort.

Job rotation
The process of *job rotation* is usually implemented as part of human resources (HR) management plan to rearrange and reallocate personnel among numerous jobs to provide a breadth and depth of experience in the various interrelated duties. Job rotation allows qualified employees to gain insight into the inner processes and workings of an organization, reduces individual boredom and stimulates satisfaction through routine variation.

Common Access Control Methods

All computer systems share common access control methods despite the vast difference and diversity in computing platforms, security concepts and protection mechanisms in use. Access control is the means and mechanisms by which secure access is managed and maintained in a multiple-user computing context, whether it's protected an isolated system or the complex interaction among multiple computers in a network context.

Mandatory Access Control (MAC)
Mandatory Access Control is a multi-level security that identifies people, services and systems as *subjects* and all other resources as *objects*. MAC uses subject and object labeling called *security labels* to define the role, responsibility and rights for those entities on a protected system. Subject access is restricted based on the sensitivity of the information contained in objects and the formal authorization or *clearance* level of that subject.

Security labels
Remember, MAC defines entities (i.e., users, systems and services) as subjects that are granted certain access rights or clearance levels. In a MAC environment, permissions are not controlled by an object's owner but instead defined by the rules of a security policy. Each object is given a security label defined by a clearance level (e.g., Confidential, Classified, Secret, Top Secret). If the security labels of subject and object do not match, then access to the protected object is explicitly denied.

Types of MAC
MAC is divided into two separate forms:

- **Non-Universal MAC**: A subject has no restrictions placed on it by default. Restrictions are placed by adding policies and defining access levels.
- **Universal MAC**: A subject is limited by default, and access policy is explicitly granted.

Discretionary Access Control (DAC)
Discretionary Access Control is a simplistic means of restricting access to objects based on subject or identity or group membership. DAC is discretionary in that object owners can pass permission unrestrained (even indirectly) onto other subjects. Under DAC, ACLs are applied to system resources (e.g., files and folders) that define the permissions users (or subjects) have.

File ownership
Subjects that create objects are implicitly granted full permission to those objects. All other subjects must be granted permission by the object's owner to access and modify its content. Ownership attributes are tracked by the file system, operating system and various applications to further enhance and enforce DAC permissions.

Role-based Access Control (RBAC)
A *role-based access control* model defines permissions according to job roles that determine an individual's or group's ability to access data or system resources. RBAC is used interchangeably with *non-discretionary access control* and forms a third complementary solution to both DAC and MAC. A basic ACL forms the most common basis for RBAC.

Role-based access control takes a secure approach to controlling access that is easiest to manage and maintain because the access controls do not require modification as individuals assume new job roles and responsibilities.

Rule-based Access Control (RBAC)
A *rule-based access control* model—which contracts to the same abbreviated form as *role-based* access control, creating some confusion—allows or denies access to objects based on a set of administratively-defined rules. Like DAC, rule-based access control maintains security attributes in ACLs associated with each object.

Subjects attempting to access protected objects the ACLs for that object are consulted before granting any form of access. Rule-based ACLs may block resource access during certain periods or within scheduled blocks of time throughout the weeks and months (such as restricting network access after hours). Like MAC, the ACL permissions cannot be assigned and administered by object owners.

Note: Abbreviated forms for both role-based and rule-based access control create confusion and conflict. Always clarify which form is represented in the context of a security conversation to eliminate all doubt and stifle any confusion.

User and Computer Security Role Assignments

Use several interrelated concepts you've learned in this and previous chapters to define, describe and detail individual end-user, collective group and endpoint computer security roles. Each of these roles are written into policy and exercised in practice to determine individual and group responsibilities within the organization (e.g., first responders, network administration, disaster recovery planners), then implemented in the protected computing environment.

For example, Windows-based network domains allow the creation of local and global user and group accounts. You assign individual or collective permissions to resources and assign rights to perform certain tasks on either local, global or both levels. Computers membership in a given workgroup allow unified access across multiple systems using a single domain account rather than having several separate local user accounts.

Comparison and Implementation of ACL Methodologies

Access control lists, filtering rules and security policies form the basis for organizatioanl security protocols, procedures and programs. Many implementations fall into one of the following basic categories and though most operate stand-alone they're all best practiced as components of a much larger security framework.

Access control lists
An *access control list* forms the most basic security checklist against which permitted accesses and actions are evaluated. ACLs define which actions a subject may take when accessing, creating, executing or modifying a given object (e.g., applications, data, processes, services). Administrators define basic permission schemes that determine how users interact individually or collectively with a protected resource.

Group policies
A *group policy* provides centralized control over system configuration and management, defined as collections of administratively-defined user environment settings. Group policies collectively define the interactions and interconnections between users and systems, including fine-grain aspects such as password policy timeouts, account lockouts and retry thresholds, and password expiration periods. Use group policies to enforce overall company and security policies through the appropriate technical and mechanical controls.

Password policies
Strong password attributes are a crucial deciding factor in the security equation. Weak passwords leave even the strongest systems vulnerable to automated attack and most users are either unaware or uneducated in making strong choices. A *password policy* establishes the standards by which all passwords are upheld, defined by organizational guidelines and viewpoints on improving password security, maintaining end-user awareness and continual policy enforcement.

Domain password policies
Windows-based Active Directory domains benefit from a Group Policy administered globally among networked systems. Domain password policies govern the password criteria (e.g., history enforcement, password aging, minimum length and complexity requirements) for an entire domain of computers.

Account credentials (usernames and passwords)
Authentication is generally based on credentials, such as Username and Password. To be authenticated, you need both pieces — the Username and the Password. By example, Windows 2000 and Windows 2003 support passwords up to 127 characters. They have the following capabilities for enforcing a good password policy:

- **Enforce Password history:** Passwords should be changed on a regular basis. By that same rule, users should not be permitted to use the same few passwords over and over again.
- **Maximum password age**: In order to ensure that users change passwords on a regular basis, policy must determine how long accounts are permitted to use the same password. If this is set to zero, passwords will never expire.
- **Minimum password age:** The purpose for requiring a minimum password age is to prevent users from using their favorite password until it expires. It also prohibits them from changing their password more times than the system remembers, and cycling back to their favorite password—thus circumventing the system.
- **Minimum password length**: The length of a password is one factor that determines the difficulty and time required to "crack" it.
- **Password must meet complexity requirements:** Passwords are made up of various characters, which can be broken down into four character groups. These character groups are: uppercase alphabetic, lowercase alphabetic, numeric, and special characters. Requiring complex passwords will require new passwords to use characters from three of the four groups.

Time-of-day restrictions
Contemporary network access policies are typically enforced through *time-of-day restrictions* that specify a certain period during operational hours when authorized users may access the Internet or certain aspects of the LAN. Time constraints curb after-hours network interactions and contain traffic activity in manageable periods.

Account expiry
Maintaining hundreds to thousands of user accounts is a complex management challenge carrying a significant security impact with either positive outcome or negative consequence. Old user accounts that go dormant often become the target of attack because intruders are sure of two things: A) the account owner is unlikely to be encountered; and B) administration keeps loose watch over its subjects. Enforcing a group policy for account expiration ensures that no unused account persists (all current and valid accounts will immediately renew) and eventually all accounts will expire.

Logical tokens
A logical token or soft token are comprised of two components: 1) encoding software application that implements a one-time password (OTP) function; and 2) initial seed value used to generate OTP function output. These tokens store information necessary to authenticate individual users on protected systems. Examples include: RSA SecurID, proximity cards, electronic keyfobs and others. In most cases, the generated software token is used once only to prevent later reuse by unauthorized parties.

Summary of Authentication Methods

The term *authenticate* means to render something authentic, grant sufficient authority or entitle sufficient credit to determine as real and true. In a secure computing context, authenticity identifies a subject authorized to access a computer or network object (i.e., application resources and system services). *Authentication* is the process of factually verifying that a user or entity actually owns a claimed identity.

The term 'Authentication' entails the following:

- Authentication is the process of finding out if something is exactly what it appears to be. For example, you can be 'authenticated' into a Windows Domain based on credentials, such as username and password. The Domain authenticates you and provides access if you can correctly verify your identity and have the proper credentials.
- The weakness with authentication is the fact that if your credentials are compromised, then there is the possibility that they can be exploited by someone else.

An *authentication factor* is any piece of information used to prove or verify an identity or appearance for the purposes of obtaining security access or clearance to a protected resource. Authentication factors break down into the following categories:

- **One-factor authentication:** single-factor authentication uses one form of authentication to verify an identity (i.e., state ID or driver's license).
- **Two-factor authentication:** dual-factor authentication uses two factors (i.e., bank card and PIN) to prove a user's identity to deliver a higher level of assurance than single or one-factor authentication.
- **Multi-factor authentication:** three or more factors used to prove an identity provides the strongest form of authentication possible, but at a higher implementation and maintenance cost than any other form.

Authentication methods fall into one of several categories:

- **What you know**
  This is the most common type of authentication method. Your password is what you know. The computer bases its authentication on the password. If you give your password to someone else, the computer will grant that person access because the authentication is based on their knowledge of the password.
- **What you have**
  This is a more advanced type of authentication. In this case, you need some physical item for authentication. An example is a building entry card. Anyone who has the card and moves it over the card reader will be granted access to the building. Here, authentication is based on what you have. If you want to have a stronger authentication mechanism you should incorporate an additional component of "what you know," such as the pin of the card. This then becomes a two-factor (**multi- factor**) authentication method. An example of a two-factor authentication method would be a smart card. You must have the smart card, as well as know the pin that authenticates you via the smart card.

  Smart cards contain integrated circuit chips with memory and processing capabilities to store personal information about a user. It provides dual authentication with the use of a card reader.

Smart cards themselves are not passwords, but may require a simple PIN-based password for access to the certificate or other data stored on that device.

Token devices are also considered an example of the "What you have" type of authentication factor. Please see the discussion on token devices later in this exam manual.

- **Who you are**
  Biometrics is an example the "Who you are" type of authentication. Biometric-based authentication is considerably more accurate than current methods. It links the verification process to an individual, not to a card, account number, PIN, or password. A biometric cannot be shared, forgotten, or lost. The process is automated instead of relying on manual verification. Fingerprint, retinal eye scans, and voice analysis are some common biometric authentication methods.

Single sign-on (SSO)
The *single sign-on* access method enables users to log in once and gain access to multiple systems without being prompted to enter credentials any further. Different applications and services support varying authentication mechanisms, so SSO provides the translation layer to store and match against the various credentials among these differing implementations.

Common SSO configurations use Kerberos, smart cards, tokens and certificates.

Authentication Model Components and Deployment

Authentication is the process of proving a claimed *identity*—that of a trusted individual or organizational entity. Forms of proof and methods of verification widely vary to match the durability and strength required by authentication and the sensitivity level of protected assets. Many of the forms introduced below operate in conjunction with other secure processes and procedures to establish a proper authentication framework suitable for local and remote connections.

Biometric reader
Among the latest forms of authentication is *biometrics*, which measures biological data samples and recording of individual characteristics to uniquely identify authorized persons. Biometric readers sample various forms of biological data (e.g., fingerprints, retinas, voices) in search of distinguishing features that provably verify a user's identity.

Remote Authentication Dial-In User System (RADIUS)
Authenticating remote entities is a different challenge than when dealing with local users and groups. The Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol that manages and maintains user profiles in a centrally-administered database that provides protective connectivity for guarded resources. RADIUS is often used in dial-up user connections and enterprise-grade wireless authentication setups to authenticate users, authorize access and enable communications with internal computers, servers and network devices.

Remote Access Server (RAS)
Remote Access Servers (RAS) are systems that allow you to connect to a server, usually via modem, to be authenticated. If you are authenticated, then you can have remote access to local system files you are authorized to use. Since RAS systems are publicly accessible system, you need to add them to your list of auditable systems.

Lightweight Directory Access Protocol (LDAP)
The *lightweight directory access protocol* is an application protocol used to query and modify TCP/IP directory services, or sets of objects organized into a logical hierarchy. LDAP organizes organizational resources into a directory tree that branches into entries representative of people, organizational units (OUs), network objects (e.g., printers, storage), and documents. Like a telephone directory keeps categorical entries of individuals and businesses, LDAP maintains a similar resource for categorizing and enumerating computer-related assets.

Remote access policies and remote authentication
An organizational remote access policy establishes the basic criteria and baseline standards that are required for remote and roaming authentication into the guarded network. These criteria and standards minimize the potential exposure to resultant damages from unauthorized usage, including the loss of sensitive information, compromised intellectual property, tarnished public image, internal system failure, or imposition of financial responsibility. Remote access policy defines how subjects may access all objects on the network during remote authentication and under what terms and conditions such access is granted.

Virtual Private Networks (VPNs)
A *virtual private network* (VPN) establishes cryptographically secure communications tunnel between private networks using the public Internet as a transmission medium. VPNs provide a secure means for remote and roaming users to accessing company servers and services. Clients and consultants may safely connect to corporate servers and VPNs can connect to other VPNs forming an *extranet*.

Kerberos authentication
For the exam, you must know the following concerning Kerberos:

- Kerberos is a very secure method for 'authenticating' a request for a service in a computer network.
- Kerberos lets a user request an encrypted 'ticket' from an authentication process that can then be used to request a particular service from a server.
- As the Kerberos system relies heavily on time stamps, the ticket you receive from the Ticket Granting Server (TGS), is time-stamped. Thus, you need to have a reliable time source available.
- Kerberos uses symmetric-key cryptography to provide single sign-on authentication.

Challenge-Handshake Authentication Protocol (CHAP)
For the exam, you must know the following concerning CHAP:

- CHAP (Challenge-Handshake Authentication Protocol) is a protocol that allows you to securely connect to a system.
- Password Authentication Procedure (PAP) is not secure like CHAP; thus, you should use CHAP instead of PAP. PAP is also very vulnerable to eavesdropping.
- CHAP uses a one-way hash function. If the hash values match from sender and receiver, then the authentication process continues and your connection is established.
- CHAP is mostly used on PPP based networks.

Digital Certificates

In cryptography, electronic documents called *digital certificates* form virtual fingerprints that absolutely identify an individuals and organizations by binding a public keys with public entities. The most common usage for a digital certificate (also called a *public key* or *identity certificate*) is for cryptographically securing HTTP transactions through HTTPS. SSL issues a server-based certificate for secure communication between Web server and client.

Certificate-based authentication may occur through logical software tokens (embedded in smartcards) to establish a trust relationship verified and validated by an independent third-party entity called the Certificate Authority (CA). Some digital certificates conform to the **X.509** standard.

Password Authentication Procedure (PAP)
The *password authentication protocol* (PAP) is a simple authentication protocol connecting end-users to network access servers as used with point-to-point protocol (PPP). PAP transmits plaintext ASCII passwords across the network and is therefore insecure, despite seeing usage as a last resort in absence of stronger authentication protocols (like CHAP or EAP).

Mutual authentication
Mutual authentication is the process of authenticating both entities in a network connection or process. An example is an IPSEC session between a client (workstation) and a server. Both the client and server mutually authenticate one another before setting up a secure connection.

802.1x authentication
Port-based network access control for wireless device authentication is provided by an international standard called IEEE 802.1x or just 802.1x for short. It relates to the 802.1 group of network protocols used among 802.11 access points and is itself based on the Extensible Authentication Protocol (EAP). There are three things you should know about 802.1x authentication.

- 802.1X is designed to enhance the security of wireless local area networks that follow the IEEE 802.11 standard.
- 802.1X allows for an authentication framework for wireless LANs.
- 802.1X allows a user to be authenticated by a central authority.

TACACS+ authentication
Remote authentication protocols take on many forms. Terminal Access Controller Access Control System (TACACS) is an original remote authentication protocol that enables a remote access server (RAS) to forward a user's credentials onto a proper authentication server. TACACS+ is an extension to this original security framework that allows users to utilize multiple factors for strong multi-factor authentication.

Differences Between Authentication and Identification

Everyone has an identity that composes indicative or signifying traits: proper names, official titles, physical attributes, established reputations, and so forth. Identity distinguishes one individual from another based on a number of characteristics including complexion, ethnicity and heritage. Through this identity other attributes are assigned: attribution of authorship, ownership and membership into authorized groups.

Identification is the act of claiming a specific identity with verifiable proof to support such a claim. *Authentication* is the process of verifying a claimed identity by validating one or more forms of proof. What we provide as identification (to prove our identity) is analyzed and considered by a person or computer (an authority) to grant or deny our authentication.

Application of Physical Access Security Methods

A comprehensive security strategy covers all boundaries whether electronic, mechanical, physical or virtual. The strongest security solutions are significantly weakened when exposed to direct attack, and insufficient physical protection is the shortest and surest path there. That pervasive defense-in-depth strategy also encompasses physical protections to site, facility, equipment and personnel.

Physical access logs and lists

A primitive form of physical access control is the *access log*, which is basically a "guest list" of individuals permitted (and sometimes expressly forbidden) access or entry. Receptionists are often called gatekeepers because they singularly allow or deny passage based upon whatever rules are under enforcement, and that usually means consulting a checklist or access log, which can keep details such as who entered where, the duration of stay or visitation, whom the person(s) came to contact, etc.

Physical access control (ID badges)

A complementary component to physical access logs are employee identification (ID) badges. IDs permit quick spot-checks of authorized credentials and are among the more primitive forms of access control. ID badges may or may not contain an employee photograph, magnetic stripe or bar code, and other anti-tampering features depending on the level of secrecy and strength of security required.

Hardware locks

Physical locks create the most basic and fundamental form of security. A hardened server sporting the latest in cryptographic and security technologies is indefensible without the security doors and locking mechanisms that safeguard the server room. There are many types of electronic and mechanical locks that suit a number of purposes (e.g., combination locks, keycard entry, biometric authentication, keyring keys), which must be chosen to fit the circumstances and conditions.

Door access systems

A *door access system* is any self-contained security system that provides physical access control to secured rooms and buildings. They typically operate in stand-alone environments, accessed by a single management computer for programming and reporting tasks. Systems may feature keypads, card readers or some biometric form of authentication for authorized entry.

Man traps

Original *man traps* were mechanical devices designed to catch poachers and trespassers, and the modern variant takes a page from that history. Modern man-trap usage employs physical access controls that restrict human passage into protected sites, facilities and rooms. In extreme cases, a series of protections might include guarded double-doors presenting differing security challenges of varying complexity and design.

Physical tokens
Any physical token is specifically a *something you have* authentication factor. The most basic and commonly understood form is the key access card and corresponding card reader that permits employee entry to an electronically-guarded entrance. Smartcards contain integrated circuitry and embedded chips, RSA SecureIDs cyclically generate passcodes and proximity cards use radio frequency (RF) transmission for physical token access.

Video surveillance
Closed-circuit television and other forms of camera surveillance provide adequate passive monitoring devices that augment existing physical access and control strategies. Video surveillance makes for an ideal witness during investigations and an unbiased observer for monitoring tasks. Units range from low-power CCDs to infrared, ultraviolet and thermal trigger systems that are becoming increasingly smaller in size for optimal placement. Video monitoring must be persistent and augmented by recording and cataloging practices to be truly effective.

Domain 4 - Assessments and Audits

IT security is encapsulated within the concept of *risk management*—a collection of methods and mechanisms designed to assess, monitor and reduce operational risks associated with organizational environments. Risk can originate from accidents, incidents and natural causes only to pose various threats to the enterprise network, corporate assets or personal safety. Risk management concentrates administrative activity to manage uncertainty, handle threats and enforce policies that ensure conformance with risk management procedures, protocols and processes.

Risk Assessment, Analysis and Management

A formal *risk assessment* process performs an objective evaluation with the end-goal of determining both quantitative (measurable quantity) and qualitative (measurable quality) values of threat and is the first phase of *risk management*—the process of assessing risk and establishing appropriate controls. The *risk analysis* portion of risk assessment attempts to identify the risk factors that prompt particular risk mitigation practices and risk management processes.

A *quantitative risk assessment* calculates risk (the magnitude of potential damage or loss) and the probability that such a consequence will occur. Risk assessment resolves assumptions and uncertainties about risk and threat into clearly considered and well-defined. Information security assesses risks through types of risks (risk categories) and how those risks occur (risk factors).

The following items cover the basis of risk categories:

- **Damage:** results in physical loss of an asset or the inability to access assets.
- **Disclosure:** revealing critical information regardless of how or where it's revealed.
- **Losses:** permanent or temporary, including the alteration of data or inability to access data.

Risk factors include the following:

- **Physical damage:** results from natural disasters or other factors, such as power loss or vandalism.
- **General malfunctions:** expected mechanical failure of system and network devices.
- **Malicious activity:** intentional acts from inside and outside the network including misuse of information, unauthorized disclosures, or attacks against informational assets.
- **Human error:** accidental and incidental occurrences, often without intention.
- **Application error:** program and operating system failures that are typically accidental, as actively exploited application errors are intentional attacks.

Risk analysis covers some of the concepts below:

- **Threat:** any present or potential source of danger; an imminent or pending event of undesirable consequence or outcome.
- **Exposure:** accidental or incidental disclosure of privately withheld information, such as unguarded.
- **Uncertainty:** characterizes the lack of confidence in the value of any element of the risk assessment.
- **Vulnerability:** a generally susceptibility to attack as applied to systemic weakness thereby violating the integrity of that system.
- **Losses:** Realized losses that occur through security exploitations.
- **Asset Value:** a measurable numerical quantity.
- **Exposure Factor:** A calculated exposure factor that occurs through liabilities being expressed to external threats.
- **Single Loss Expectancy/Exposure:** A single incidence of exposure that realizes a loss.
- **Annualized Rate of Occurrence:** The calculated rate of loss occurrences per year.
- **Annualized Loss Expectancy:** The total loss occurred per year.

Security Audits

A *security audit* is the collective means through which a risk assessment is conducted to ensure compliance of enforced organizational or regulatory security policy. Security audits challenge the mechanisms and methods used to enforce a given security policy with the end result of verifying and validating the correctness (in implementation and functionality) of those implements. Manual security assessments involve staff interviews, vulnerability scanning, application access review and operating system access control enforcement. Automated security assessments are software-driven methods of producing system-generated audit reports or establish monitoring and reporting of system changes.

Threat Management

Threat management is basically defined as the process of protecting against potential strategies and sources of attack. A proper threat management framework prevents mostly known (and some unknown) attacks against guarded company resources including both computing platforms and personnel alike. It makes every attempt to reduce or eliminate the possibility of a successful attack being conducted. To manage threat means taking extra precautions and preventive measures to altogether avoid risky behavior or situations and protecting against the probability and potential of attack to protected resources and personnel.

Vulnerability Assessments

Vulnerability scanning is the automated process of identifying security exposures, risks, threats and vulnerabilities. Original tools like SAINT and SATAN pioneered the vulnerability scanning field to assist administrators in detecting system and network vulnerabilities, the results of which are as current and relevant as the tool and its checklist database. *Vulnerability assessment* is a method of identifying, quantifying and prioritizing system or network vulnerability (as enumerated by vulnerability scanning) and naturally complements risk assessment where both catalog, identify, rank and mitigate risk starting with high-priority items first.

Port Scanners and Network Mappers

An integral aspect of a network vulnerability assessment is the *port scanner*, a software tool used to identify listening ports and (to some extent) enumerate listening services. Port scanners are the investigatory tools through which good and bad discoveries are made by administrators and intruders alike. Each port scanner varies in form, function and feature but all serve a similar purpose in locating the open portals through which most attackers attempt to make entry.

Network mappers are a higher-level learning tools that help users visualize the network *topography* or logical arrangement and layout of devices. Where a port scanner gains perspective into individual system attributes a network mapper gains a more comprehensive viewpoint into the attributes of the larger encompassing network.

Service Mapping and Vulnerability Scanners

A specialized form of security assessment, service mapping and vulnerability scanning focus on enumerating reachable network service banners and identifying vulnerable product versions based on a number of "fingerprinting" methods. Vulnerability scanning may also incorporates functionality to identify configuration and operational weaknesses. Like port scanning, service scanning identifies listening services and potential entry points for network intrusion.

Open Vulnerability Assessment Language (OVAL)

International in scope and free for public consumption, the *open vulnerability and assessment language* is an information security standard designed to promote open and public security content, and standardize the utilization of this information across various security tools and services. OVAL is a collection of XML schema for representing system information, expressing specific machine states and reporting assessment results. Use of OVAL provides a methodical examination of organizational IT infrastructure weakness to derive recommended resolutions to control and remedy exposures to risk.

Password Crackers

Login account security's top priority risk is consistently one thing: password strength. Overall password complexity comprises a number of elements including character length, letter-number substitutions, non-deterministic vocabulary (i.e., anything but predictable dictionary words) and other contributing factors. A *password cracker* is tasked with identifying poor password choices by random or sequential retries against various dictionaries, word lists and automatically generated entries.

A user's password should never contain important information (birthdates and social security numbers) or guessable information (proper or pet names). Usually an 8 character minimum provides the strongest basis for password selection (except for high-risk environments) and should contain a mixture of alphabetic letters, numerics, punctuation and various shortenings (abbreviated phrases or acronyms) and substitutions (numbers for letters).

Penetration Testing versus Vulnerability Assessment

Penetration testing and vulnerability assessment are both crucial components of the overall security assessment framework. The most distinguishable difference is that penetration testing continues where a vulnerability assessment ends. Vulnerability assessments are discovery processes meant to identify sources of risk to system or network; penetration testing furthers this assessment by conducting live exploitive attacks against identified vulnerabilities (targets of threat and areas of risk).

Penetration testing evaluates system security by simulating malicious attacks and involves active analysis for potential system or network vulnerability—as discovered during a vulnerability assessment. Analysis and activity is conducted from the viewpoint of an attacker to provide near-realistic impact. Technical solutions are provided for both testing and assessment phases, but only penetration testing takes active measures to validate assessment results.

Network and System Monitoring Tools

Exploits to network devices and network operating systems are common, numerous, and constantly recurring. Administrative upkeep for corporate networks scales with respect to its scope and size, but the most constant elements across all environments are the monitoring tools used. Various performance and reliability monitoring tools trace performance and track issues across operating systems and network devices. The practice of IT security demands familiarity with basic toolbox implements, the most common of which are described below.

Systems Monitoring

System monitoring oversees daily activities, events, and incidents related to individual endpoints—as opposed to monitoring collective and individual network interactions from a network-centric viewpoint. System monitoring devices range from integrated performance, reliability, and monitoring tools covering various applications, services, and user interactions. Log files are typically consulted to track-down performance and reliability issues, identify sources of intrusion, and correlated system-wide events from specific endpoint stations. Monitoring individual systems in large scale environments can easily become unmanageable, so it's prudent to choose comprehensive solutions that are capable of analyzing and summarizing reports and results, thus easing administrative workload.

Performance Monitor

Keeping watch over system performance gives great insight to its overall health and wellbeing. A well-behaved system in great health encounters little unscheduled downtime, interruptions and shutdowns (defining a baseline of known-good behavior). Behavioral anomalies such as after-hours or spurious reboots, faltering performance or unauthorized configuration changes can signify an intrusion—or at least some questionable activity worth investigating.

Performance Baselines

A *performance baseline* is the metric benchmark against which ongoing system performance is measured. Baseline performance monitoring involves establishment of charted chronological performance accompanied by an interpretation of those results based on specific considerations of the monitored environment. Many elements of that chart (such as timeframe) vary according to environmental constraints and conditions. Performance baselines are applied to applications, processes, operating systems, server services, and network interactions.

Protocol Analyzers

Network protocol analyzers or "packet sniffers" set a workstation's network interface into *promiscuous mode*, which is a more permissive state allowing the network stack to process packets destined for other computers—packets normally filtered out by the NIC. The sniffer acts like a viewfinder into network traffic patterns and protocols enabling administrators to observe private conversations, sensitive transactions, and special relationships between other computers for investigatory or troubleshooting purposes. In the wrong hands, protocol analyzers can permit eavesdropping and interception of sensitive protocol transactions.

Monitoring Methodology Comparison and Contrast

Monitoring networks and systems against an ever-expanding array of infections and intrusions is a difficult undertaking that requires a collection of independent software components and concepts. Each method of managing, matching, and monitoring for threats and malware is performed with varying advantages and disadvantages for certain conditions, circumstances, and criteria. Best practices show that deploying multiple overlapping technologies provides the most comprehensive coverage one can expect of a secure environment.

Signature-Based Engines

A *signature*-based algorithm (also called *pattern matching*) examines application activity and network traffic for signs of attack or malware. Known attack methods impart certain patterns that are formatted into signatures for easy identification in streams of running applications, servicing services, and protocol payloads. Some scanning engines are even designed with flexible signatures capable of matching changes and variations to original malware.

Signature-matching algorithms are only capable of detecting *known* attack methods; new or existing and uncatalogued attacks or malware are likely to go unnoticed. Such algorithms require large, updated databases of signatures to match against the growing scope and scale of threats against systems and networks. As the size of that database grows and the scope of the scanning expands, processing time and resource utilization increases accordingly.

Anomaly-Based Engines

A *heuristics*-based algorithm (also called *anomaly* or *behavior* detection) is a self-learning, rule and/or weight-based method that produces acceptable detection results in practical situations where no formal proof of correctness exists. Heuristics algorithms analyze current application or network behavior in search of questionably deviant activity (anomaly) from known-good history (baseline) Scanning methods are based on intelligent search strategies using alternative approaches to seek instructions or commands that signify potentially malicious behavior and is able to detect malicious functionality in new, previously unexamined malware.

Anomaly-based matching is prone to false positives where normal code changes or behavioral variance is misidentified as a malicious attack. Heuristics possesses an intensely analytical nature can hinder performance on busy systems and take time to "learn" an application's or network's baseline.

Audit Trails and Logging Procedures

System auditing and logging are crucial aspects to maintaining tabs on policy enforcement and electronic paper trails on application, process, and user interactions. Financial, governmental and healthcare industries are especially regulated fields that require heavy accountability and demand strict compliance. Audit trails and logging procedures are the key elements to establishing and maintaining the accountability relationship between subjects and objects. They're also instrumental to correlating network intrusions to help recreate the scene of events.

Security Application

An *audit trail* is any series of records detailing computer events involving application, operating system, and end-user activities. Audit trails maintain records for system activity in terms of application processes and user actions. In conjunction with other security tools and procedures, audit trails facilitate the detection of security violations, performance issues, and other suspect interactions. A single system may utilize several audit trails devoted to particular activities—not all of which may be security related—to enable full analysis and review of management, operational, and technical controls.

Domain Name Service (DNS)

The openness of DNS has made it the subject of various attacks that vary in frequency, intensity and sophistication. DNS can potentially reveal an entire organizational footprint including network devices, service versions and server roles. An organization's name servers require substantial auditing and assessment to identify weaknesses and detect vulnerabilities. Inconsistencies in domain reversals (name-to-IP and back), zone transfers, RFC non-compliance, and outdated software versions are just a few issues plaguing public-facing DNS.

System Access and Performance

Log files for system accesses and system performance illuminate areas where instability and intrusion leave traces of evidence. From an end-user standpoint, a misbehaving application may appear no different than an exploited application on the surface, but telltale signs are left behind in associated log files. Use log files as your viewfinder into diagnosing, identifying, and troubleshooting system issues and also system intrusions.

Firewall and Antivirus Logs

Another crucial correlation factor following an intrusion is located in antivirus and firewall logs. These two sources provide details on network access interaction and local host interaction (unless the antivirus is located centrally like a network-wide spam filter) both capable of yielding great insight to system faults and failures. Pay particular attention to antivirus application shutdowns (or update site redirections specified in the hosts file) that are not user-initiated, which is a signature for newer malware that prefers to avoid detection by eliminating the detection methods themselves altogether.

Periodic Audits of System Security Settings

Pilot testing programs establish validation tracks for evaluating changes prior to implementing them in a production environment. System security settings require periodic follow-up audits to ensure no subsequent configuration changes adversely affect previous settings and that original changes remain constantly valid. Collective policies, procedures, and processes related to system security settings should also undergo periodic review.

User Access Rights and Review

Pilot testing programs are established prior to production environment roll-outs because we fallible humans don't always get things right the first time around—and sometimes it even takes several subsequent failures and retries before succeeding. The complementary ongoing maintenance phase is periodically reviewing and validating such changes and introductions to ensure that all objectives are met and no new issues arise or existing problems persist. Periodic user access rights review helps you identify where these issues occur and ensure that—once corrected—they never return.

Data Retention and Transmission Policies

Certain governmental laws and federal regulations apply to sensitive data retention and transmission related to financial institutions, healthcare systems, and governmental organizations. Under these circumstances storage and retention policy establishes secure procedures for storing and transmitting confidential client information, electronic commerce exchanges, private patient records and other forms of sensitive or personally identifiable information. Even archived e-mails, logged instant messages, and backed-up user files may qualify as sensitive or personal information worthy of protection.

Strong data retention and transmission policies guide organizations in protecting such valuable information assets to avoid financial, civil and criminal penalties for non-compliance with federal laws, governmental mandates and industry regulations. These regulations, mandates and laws dictate how data is stored, permissible media storage, storage duration and what protections and auditing mechanisms should be established for best results.

Group Policies

Group Policy provides centralized management and configuration of local and remote computers and users operating in a domain environment. Performing a pilot test prior to rolling out changes or configurations to a production environment ensures fewer unforeseen side-effects and provides last-minute tuning prior to launch. Pilot testing is a three-part process consisting of the following: 1) ensuring group policy enforces restrictions or functions as expected; 2) noting significant errors or implementation issues and adjusting calculations or configurations accordingly; 3) addressing any unexpected errors as they arise.

Domain 5 - Cryptography

The application of cryptography—the discipline and application of concealing or disguising information—has been around for centuries, but only since the age of secure computing has its true potential been revealed. The field of computer cryptography encompasses many concepts, constructs and components that vary from simplistic to sophisticated. Usage and understanding of the principles, properties and protocols is essential for earning Security+ certification and necessary for becoming a paid security professional.

General Cryptography Concepts

Cryptography is the formal practice and study of concealing or disguising information. *Encryption* is the process of converting ordinary information (or *plaintext*) into unintelligible data (*ciphertext*). The reverse process of converting ciphertext into plaintext is called *decryption*. Cryptographic algorithms are the software components that drive encryption and decryption, which often uses a cryptographic key to prevent simple analysis of encrypted data.

Cryptography is a richly-populated field full of tactics, techniques, and traditions. As a Security+ practitioner, you must possess a firm comprehension of cryptographic principles and firm understanding in their practical applications. Cryptography is the science and practice of concealing confidential messages; *cryptanalysis* is the science of analyzing and deciphering those messages.

Hashing

The cryptographic *hash* function takes an arbitrary block of data and produces a fixed-size string called the *hash value* for later verification. The resultant hash value ensures that once data is received it has not been altered at any point between sender and recipient. Hashes provide message integrity checks, digital signatures, secure authentication, and various information security applications. Hashing is considered a one-way function because the resulting hash value is useless in reconstructing the arbitrary data it was created from originally.

Example hashing algorithms include:

- **Hash of Variable Length (HAVAL):** produces hashes of differing lengths including 128, 160, 192, 244, and 256 bits. HAVAL allows user-specified rounds (3, 4, or 5) for use generate the hash.
- **Message Digest:** a family of widely-used algorithms (MD2, MD4 and MD5) producing a 128-bit hash value that has proven not to be collision resistant. However, it continues to see use as an integrity checking algorithm.
- **RACE Integrity Primitives Evaluation Message Digest (RIPEMD):** an early (circa 1996) 160-bit message digest algorithm that uncertain security implications with regard to hash collisions and overall security.
- **Secure Hash Algorithm (SHA):** a family of identical algorithms (though differently structured) producing a variable-length digest. SHA is employed widely in security applications and protocols.

Steganography

Security through obscurity is generally an ill-advised security practice, but *steganography* is exactly that: an encryption method that encapsulates messages, obscuring them from view so that only sender and recipient are aware of its existence. Steganography most commonly conceals information within unassuming computer files: audio, photo and video formats are prime choices, and other documents or text-based files work as well. While cryptography disguises the meaning of a message, steganography disguises its presence to drawing attention and avoid detection.

Symmetric Key

Symmetric key cryptography (also called *shared-key* or *private-key* encryption) algorithms use identical or similar encryption keys for processing encryption and decryption. Encryption keys may be trivially related in that they're exactly alike or simply transformed for slight variance. Both keys represent a *shared secret* between two or more parties used to maintain a private conversations and confidential communications.

Block and stream ciphers
Symmetric key encryption provides to classes:

- **Stream Cipher:** A symmetric cipher in which the plaintext digits are combined with a pseudo-random cipher bitstream. Each plaintext character is encrypted serially and singly. Transformation of successive digits varies during encryption and is dependent upon the current state of execution.
- **Block Cipher**: A symmetric cipher that operates on fixed-length groups of bits (termed blocks) with constant transformation. A block cipher might consume a 128-bit block of plaintext as input and output a corresponding 128-bit block of ciphertext. Exact transformation is controlled using the secret key. Decryption is similar in that the decryption algorithm takes a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext.

Examples of symmetric key algorithms include: DES, 3DES, RC2/RC4/RC5/RC6, IDEA, AES (Rijndael, MARS, Serpent, Twofish) and blowfish.

Asymmetric Key

Asymmetric key cryptography secures private communications between parties without the exchange of secret or shared keys and instead uses separate keys for encryption and decryption routines. Similar but separate *public-key* cryptography is a subset of asymmetric cryptography that uses public and private key pairs. Keys used to encrypt messages (private) vastly differ from keys used to decrypt messages (public). However, only the public key is ever distributed or published; the private key remains sole ownership of the respective party. Despite both keys being mathematically related, it's infeasible and improbable to derive the private key from the public key (as is the case with symmetric keys).

Examples of asymmetric key cryptography include: Diffie-Hellman Key Exchange, RSA, DSA, El-Gamal, and elliptic curve.

Key Management

Cryptographic *key management* includes all provisions related to the generation, exchange, storage, safekeeping, usage, vetting and replacement of cryptosystem keys. Included in this comprehensive design are cryptographic protocols, key exchange services, user procedures, encryption algorithms and other integral components. Key management encompasses the practices, protocols and platforms used to enforce, exchange and execute these various functions and services.

Confidentiality, Integrity and Availability

Three concepts comprise the CIA triad: confidentiality, integrity and availability. Combined, these concepts form the basis of well-designed security architectures, frameworks and platforms. When designing a security control infrastructure, the ultimate objective should be to provide controls for these three elements. The following are common definitions of these terms that can be applied to assess security risks:

- **Confidentiality:** Confidentiality prevents sensitive information from being disclosed to unauthorized recipients. The intent is to reduce or eliminate the risk of financial loss, public embarrassment, or legal liability from unauthorized disclosure of sensitive or critical information.
- **Integrity:** Integrity ensures that information resources are changed only in a specified and authorized manner. In this case, the goal of security is to reduce or eliminate risk to the business if critical information is accidentally or intentionally manipulated or corrupted.
- **Availability:** Availability ensures that systems operate promptly and service is not denied to authorized users. The risk to the business takes the form of missed opportunities or interruption of operations because of the inaccessibility of information.

Non-Repudiation

Accountability is a crucial factor in computer security generally and computer cryptography specifically. One way to provide *non-repudiation* or undeniable proof of authorship is to digitally sign communications, documents, and messages with a private key. Non-repudiation ensures that a party cannot refute the authorship, delivery or validity of a digitally-signed article. Its meaning and application in computer security defines services that provide proof of integrity and origin of data, and also assured genuine authentication.

Digital Signatures

A *digital signature* is an electronic identifier derived from public-key (asymmetric) cryptography used to authenticate a message and give undeniable proof of authorship by the author/sender. Digital signatures are easily transportable, difficult to forge and conceal various data including contracts, email, and messages sent across the network. Private keys are used to create digital signatures (providing ownership) and a secure hash of the entire document or message is signed so that any change to content invalidates the signature (providing integrity).

Comparative Strength of Algorithms

The various forms of cryptography all perform differently: some are easily circumvented whereas others are resistant to highly-sophisticated attack. The ability for a cryptosystem to protect information from the various types of cryptographic attacks and analysis is called *cryptographic strength*. This strength depends on several factors including:

- Secrecy of the cryptographic key(s)
- Cryptographic key strength
- Resistance to breakage without use of keys
- Lack of alternate (back door) decryption methods
- Inability for any portion to be decrypted knowing some content

The ultimate goal of a cryptographic design is to produce ciphertext that cannot be broken giving complete understanding of the algorithm, its operation and its results. Cryptographic strength includes the ability to resist decryption even when the attacker already knows some of the plaintext.

Attacks against cryptography include: brute force and word variations, codebook and plaintext attacks, differential and linear cryptanalysis, man-in-the-middle attacks, and related-key cryptanalysis (just to name a few). There are also side-channel attacks that target timing mechanisms or exercise cryptographic functions in unusual ways to derive secrets or defeat systems.

Use of Proven Technologies

Computer security delicately balances controls and countermeasures against engaging threats and risk to achieve a favorable defense strategy. The use of proven technologies ensures the highest level of capability and confidence in such a security strategy and significantly increases positive results. A cryptographic algorithm that has never seen widespread use or undergone serious scientific analysis has not proven itself viable in the take-no-chances world of IT security. Likewise, other unproven access control, security monitoring, or other threat mitigation strategies should never be relied upon to secure a modern computing environment. However, an unproven technology is entirely welcome in developmental labs under pilot testing programs that attempt to ascertain a security component's viability before deployment in the production environment.

Whole-Disk Encryption

Data-at-rest describes stored information. Data at rest becomes data at risk when sensitive information is exposed or revealed in original format, unprotected by cryptography. Credit data, medical histories, and all other forms of personally identifiable information (PII) have all been headline keywords because of massive consumer, client or customer data theft affecting thousands at a time. The core issue is that in many cases confidential, proprietary, or sensitive data is either left unguarded (not encrypted) or safeguarded by incomplete cryptosystem implementations. Then it comes into contact or falls into the hands of thieves (usually stealing the hardware) and potentially endangers affected individuals in financially or personally victimizing ways.

Whole-disk encryption (also called *full disk encryption*) generically describes the feat of encapsulating an entire operating system and all its related content across an entire storage volume. Whole-disk encryption signifies that everything is cryptographically protected including applications that encrypt bootable operating partitions and decrypting them at run-time. Swap spaces, temporary files, and everything created within that storage volume are entirely encrypted and not left to end-user discretion.

Full disk encryption provides several benefits:

- **All-encompassing encryption:** no file is left unprotected, even unintentionally, as anything could potentially reveal confidential information (e.g., memory-to-disk swaps, unencrypted temporary files, open documents). No more exposed data-at-rest.
- **Boot-time encryption:** certain cryptosystem implementations permit boot-time encryption, which usually provides a miniature pre-boot environment to initialize the encrypted volume before kicking off the actual bootstrapping procedure.
- **Pre-boot authentication:** a BIOS extension or boot firmware that guarantees secure, tamper-proof environments and entrusted authentication layers. PBA prevents any data from being read on a protected hard disk until sufficient credentials are provided.

- **Instant data destruction:** simply destroying the cryptography keys renders contained data useless, but proper data scrambling and data purging procedures may apply to high-risk, high-security environments.

Trusted Platform Module (TPM)

In computing, the *trusted platform module* is both a published specification detailing a cryptographic hardware system and the general implementations build upon that specification (called *TPM chips* or *TPM security devices*). TPM offers facilities for secure generation of crypto keys, usage restriction, and a hardware-based pseudo-random number generator (PRNG).

Perhaps most significantly, TPM enables *remote attestation*, which creates a nearly unforgeable hash key checksum of its own hardware and software configuration, ensuring that it has not been altered, changed or modified. It's also capable of *sealed storage* data encryption that may only be decrypted if TPM releases its associated decryption key, which is only provided to software supplying the same password the TPM chip was originally configured to use.

Single Versus Dual-Sided Certificates

As a Security+ practitioner, you should understand the basic difference between single-sided and double-sided certificates. A *single-sided certificate* allows only a client browser to identify itself with a server. However, enterprise-grade environments may demand mutual authentication between parties, which requires a *double-sided certificate* that authenticates client and server in an SSL transaction. This mutual or two-way authentication means that both computing endpoints must prove their respective identities to ensure a fully trustful interaction.

Hashing and Algorithmic Application

Many cryptographic functions, services and protocols rely upon hashing algorithms that create checksums of data for integrity verification purposes. One surefire way to ensure reliable, tamper-proof transmission between sender and recipient (whether tampering is human or machine is irrelevant) is through hashing or checksumming techniques. Hash strengths and solutions come in many varieties, some of which are provably vulnerable to calculate attack and others have yet to be "broken".

Secure Hash Algorithm (SHA)

The *secure hash algorithm* is a set of cryptographic functions originally designed by the NSA and later revised and published by NIST as a federal information processing standard (FIPS). SHA is a checksumming algorithm capable of producing fixed and variable digest sizes up to 512 bits. SHA algorithms are differently structured and distinguished as SHA-0, SHA-1 and SHA-2, the latter of which uses variable digest sizes (e.g., SHA-224, SHA-256, SHA-384, SHA-512). SHA-1 is based on principles similar to MD5 but uses a more conservative design.

Proof that certain forms of SHA is broken shows that collisions occur in fewer hash operations than brute force attacks based on hash length. That means cryptanalysis can reveal hash collisions in less time and effort than it takes to exhaustively iterate over the entire key space (in bits) of a given SHA algorithm, which means compromises its integrity and invalidates it for high-risk security usage.

Message Digest 5 (MD5)

Message digest algorithm 5 is a widely-used Internet standard (RFC 1321) hashing function that produces a 128-bit hash value expressed as a 32-character hexadecimal product. Though commonly used to check the validity of critical system files, it also serves anti-tampering functions for digital certificates, obscures password entries, verifies downloaded content and secures network transmissions.

It has been provably demonstrated that MD5 is not collision-resistant to a number of attacks and is therefore unsuitable for applications relying upon this feature (such as file integrity checkers). Two files of differing content and construction can indeed share an identical MD5 checksum and it's also possible to forge SSL certificates that pass validity checks. Extra care and precaution must be taken when using MD5 algorithms and applications in high-risk security contexts.

LAN Manager (LANMAN)

Microsoft's proprietary *LAN Manager* is an obsolete challenge-response authentication protocol used prior to Windows NT and subsequently replaced by *NT LAN Manager*. The algorithm is particularly vulnerable in that inadequate algorithmic strength allows simple brute force attack. LANMAN is a network operating system (NOS) and uses the server message block (SMB) protocol built upon NetBIOS Frames. It has been replaced by subsequent replacements but remains in use wherever original NT networks are operational.

NT LAN Manager (NTLM)

The *NT Lan Manager* succeeds and replaces the original LAN Manager SMB-based remote access authentication protocol and is similar to Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP). NTLM is also proprietary and employs a challenge-response sequence to negotiate secure channels between clients wishing to authenticate and servers requesting authentication. NTLM allows clients and servers to negotiate secure parameters and request or require supported features.

NTLM challenge-response follows this format:

- **Type 1 message:** client sends a message that contains attributes flagging requested or supported features.
- **Type 2 message:** server sends a reply containing a similar set of flags supported or required by the server (negotiating connection parameters) and a random challenge.
- **Type 3 message:** client calculates response based on Type 2 message challenge, the method of which differs according to negotiated NTLM parameters, then issues the final message.

Encryption and Algorithmic Application

Cryptography has several derivative functions and components that perform any number of tasks from securely storing and erasing information, safeguarding sensitive transactions, ensuring trusted connections between authentic parties, and so forth. Many of these applications resolve to similar design concepts and algorithmic components at the operational level and it's your job to apply and understand these concepts in the security field. Basic and common computer encryption concepts and components appear in the following paragraphs.

Data Encryption Standard (DES)

The *data encryption standard* is a deprecated 56-bit block cipher once used internationally, but has become obsolete by simple algorithmic attacks and bested by more robust algorithms and methods. As of 1999, DES was collaboratively broken by a team of security researchers forever casting DES into the annals of antiquated encryption algorithms. DES serves mostly historical purpose as one of the first and foremost block cipher encryption standards.

Triple Data Encryption Standard (3DES)

As a follow-up to its provably broken precursor, Triple DES builds upon the same 56-bit cipher but enlarges that key space without code alteration or algorithm switch. Additional cipher rounds and steps are essential to preventing attacks against basic DES and can operate with variations to number of keys used and the order of operations performed. Generally speaking, 3DES with three keys has a 168-bit key length but is effectively provided only 112-bit strength due to algorithmic shortcomings and generally slow computational performance. 3DES is itself disappearing from use in favor of more resistant algorithms such as AES.

Rivest-Shamir-Adleman (RSA)

The *Rivest-Shamir-Adleman* algorithm (named for its authors) is a foundational cipher that pioneered the first practical application and programmatic implementation of public-key cryptography. RSA is used for encrypting messages and generating digital signatures and continues to operate industrial-strength security applications and protocols like PGP, SSH and many others. Public and secret keys are derived from the factors of very large, dynamically computed numbers. RSA generally combines a padding scheme—additional or modified data used to further vary encryption—to prevent a number of known algorithmic attacks against it and defeat cryptanalysis on resulting ciphertext.

Pretty Good Privacy (PGP)

Pretty good privacy is a cryptographic application used to encrypt and decrypt e-mail for transmission across the public Internet. It's free for single-user usage and commercially sold to corporate environments (comprising multiple users) and represents a complete public-private key cryptosystem capable of protecting stored files, exchanging digital signatures and providing secure authentication. PGP employs several algorithms including DSA, RSA, MD5 and SHA to provide the services that support data encryption, user authentication, message integrity, and key management.

Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography is an approach to public-key cryptography that is based on the algebraic structure of elliptic curves over finite fields. ECC operates on smaller keys than traditionally-used RSA for more efficient performance. It also offers considerably greater security for a given key size and more compact implementations for a given level of security.

Advanced Encryption Standard (AES)

The *advanced encryption standard* comprises three block ciphers (AES-128, AES-192, AES-256) adopted from a larger collection. AES operates quickly in software and hardware implementations and requires little memory usage for operation. As a NIST Federal Information Processing Standard (FIPS) AES has passed a rigorous five-year standardization process where competing designs were evaluated for fitness until an appropriate selection was made, and is now among the most popular ciphers used in symmetric key cryptography. The different block cipher specs represent fixed-size increases and decreases to corresponding block sizes and corresponding cryptographic strength.

One-Time Pad

Cryptography includes the *one-time pad* encryption algorithm that combines plaintext input with a random key or "pad" of equal length and used only once. Modular arithmetic—a system designed for integers where values wrap around after reaching a certain maximal value—combines both aspects into the final encoded output. In a binary arithmetic format, the exclusive-or (XOR) operation performs the same task. One-time pads provide perfect secrecy whenever the generated key is truly random, kept secret and never reused.

Transmission Encryption (WEP/WPA, TKIP)

With the advent of wireless computing comes an entirely new class of cryptographic protocols for securing consumer-grade and enterprise-level communications alike. 802.11 wireless transmission suffer from unique weakness and vulnerability associated with data-bearing radio communications and require specialized encrypted transport protocols to ensure confidentiality and privacy remain inviolable, as with every security.

Wireless transmission schemes include the following:

- **Wireless Application Protocol (WAP):** a common transmission protocol between mobile phones, PDAs, and handheld computers. WAP can occasionally transmit long distances for display to small-screen displays. Specially-tailored low-bandwidth web, email, and multimedia playback are common uses.
- **Wireless Transport Layer Security (WTLS):** a TLS-based transmission security encapsulation developed to address mobile computing environments. WTLS encrypts messages between WAP endpoint and gateway, which then decrypts and repackages the message using SSL/TLS before sending to its final destination.
- **Wi-Fi Protected Access (WPA):** WPA and WPA2 are certification tracks established to indicate compliance with Wi-Fi Alliance protocol to secure wireless networks. The WPA protocol introduces TKIP (see below) and uses designated *personal* and *enterprise* modes to indicate different modes of operation.
- **Temporal Key Integrity Protocol (TKIP):** a security enhancement for wireless transmissions to strengthen resistance to brute force attacks that broke WEP. TKIP implements key-mixing functions, maintains an anti-replay sequence counter, and a 64-bit message integrity check called MICHAEL.

Encryption Protocol Implementation

Secure Socket Layer (SSL)

The *secure socket layer* is a transport layer (OSI layer 4) encryption protocol used to secure end-to-end tunnels through which HTTP or other application traffic may pass. An exemplary application is for securing electronic commerce and financial Web transactions via SSL-wrapped HTTP (HTTPS). An SSL session is *stateful* in that connection states are maintained from session initiation to connection teardown. SSL is originally developed by Netscape, but even subsequent versions (e.g., SSLv2, SSLv3) are rendered obsolete by Transport Layer Security (TLS).

Each SSL session opens with a mutual exchange of messages called the *SSL Handshake*. SSL handshaking allows servers to authenticate with clients by employing public-key cryptography methods, which in turn enables clients to authenticate with servers. Client-server connectivity continues in a cooperative fashion using symmetric keys for encryption, decryption, and message tamper-proofing. It is sole responsibility of the SSH Handshake protocol to establish and coordinate these cooperatives and perform mutual negotiations.

Transport Layer Security (TLS)

The *transport layer security* protocol obsoletes and replaces its precursor the SSLv3 protocol. TLS provides the same functionality and follows the Internet Engineering Task Force (IETF) standards track (RFC 5246), which is based on earlier SSL specifications originally developed by Netscape.

That said, TLS is not backward-compatible with SSL but does establish cryptographically secure endpoint connectivity that resists eavesdropping, tampering and message forgery. Similar authentication and communications confidentiality concepts and components also apply. TLS also supports a bidirectional authentication mode where both parties of a conversation are mutually authenticated.

TLS composes three basic phases:

- Peer negotiation for algorithm support
- Key exchange and endpoint authentication
- Symmetric cipher encryption and message authentication

The TLS protocol comprises two layers:

- **TLS Record protocol:** operates at the lowest level to provide connection security. The TLS record encapsulates data for secure exchange.
- **TLS Handshake protocol:** establishes client-server connectivity through a complex protocol exchange that defines parameters and properties for secure communications.

Secure Mail Internet Message Exchange (S/MIME)

The *secure multi-purpose Internet mail extensions* are a public-key standard for encrypting and signing email content encapsulated within MIME. S/MIME follows the IETF standards track and is defined in a number of RFCs. It provides cryptographic security services for email including: secure authentication, message integrity, non-repudiation or origin, end-user privacy and data security.

Point-to-Point Tunneling Protocol (PPTP)

The *point-to-point tunneling protocol* is an original wide-area network (WAN) protocol specification that enables the creation of network tunnels between two points and a method for implementing virtual private networks (VPNs). PPTP does not provide confidentiality or encryption and instead relies upon the encapsulated or tunneled protocol for privacy protection. Due to operational limitations and shortcomings of PPTP in an increasingly hostile network arena, its usage has been obsolete by more recent and robust follow-ups such as the layer 2 tunneling protocol (L2TP) and IP security (IPSec).

Layer 2 Tunneling Protocol (L2TP)

The *layer 2 tunneling protocol* (L2TP) is a two-component system (access concentrator and network server) that supports conventional VPN construction, configuration and communication but does not itself provide confidentiality or encryption. Instead, L2TP relies on whatever cryptographic protocol is passed within the tunnel to ensure privacy matters. The entire L2TP packet encapsulates within a UDP datagram and commonly carries point-to-point protocols (PPP), and L2TP version 3 (L2TPv3) provides additional security features, improved encapsulation, and enhanced delivery over non-IP networks.

Hypertext Transfer Protocol (HTTP) and Secure Variants

Much of the Internet's visually presentable side is made possible through the *hypertext transfer protocol*, a de facto standard TCP mechanism for exchanging content and messages between Web browsers and servers. From an end-user standpoint, HTTP provides unbounded flexibility and remarkable delivery over a range of document types, file formats, and streaming multimedia. From a security practitioner's viewpoint, such openness and variety attracts malware and malicious activity.

HTTP is an application layer (OSI layer 7) transport method that operates plaintext—every transmission is sent in original, unencrypted format and open to interception by malicious third-party eavesdroppers. SSL and TLS provide an essential security service to HTTP (HTTPS) that ensures several preventive and protective measures are taken to resist interception, manipulation or observation by unauthorized parties—particularly those placed between endpoints of a secure conversation. As a Web-based protocol, HTTPS is integrated into popular Web browsers to encrypt and decrypt page requests across TCP port 443 (instead of HTTP's usual port 80). HTTPS connections operate below the application layer to encrypt HTTP messages prior to transmission and decrypting incoming messages upon arrival.

Note: HTTPS is not identical to secure HTTP (S-HTTP, RFC 2660), an alternative though less widely-used URI scheme for encrypting Web transactions.

IP Security (IPSec)

The *Internet protocol security* suite is a network level (OSI layer 3) cryptographic framework that essentially provides two services: authentication header (AH) and encapsulating security payload (ESP). Together these services provide authentication with data integrity (AH) and encryption of encapsulated protocol payload data (ESP).

IPSec ensures secure communication in several ways:

- Provides data authenticity and integrity checking by first verifying identities between parties in a conversation. IPSec prevents IP spoofing exploits and man-in-the-middle attacks.
- Provides anti-replay protection by serializing messages with sequence numbers to ensure integrity of transmitted data on the receiving end. Captured packets cannot be later reused.
- Provides non-repudiation to undeniably prove a message's source of origin. Messages cannot be forged or ownership denied once digitally signed, sealed and sent.
- Provides strong encryption to plaintext communications protocols or vulnerable network delivery services. IPSec protects against eavesdropping, interception and sniffing attacks.

Finally, IPSec has two modes of operation:

- **Transport mode:** used between endpoint and gateways in a network arrangement, where the gateway is treated as a host computer. Plaintext Telnet sessions can be transported from workstation to router (the actual destination) through IPSec.
- **Tunnel mode:** used between gateways (such as two routers) in a network topology or between endpoint and gateway, which operates like a proxy for "hidden" hosts. Secure connectivity between branch office and corporate headquarters or home office is a typical application.

IPSec Key Management
Crucial key management functions of IPSec provide authentication, distribution and generation of cryptographic keys used to establish secure communications. The *Internet security association and key management protocol* (ISAKMP) establishes this elemental key management functionality and also incorporates mechanisms to negotiate, establish, modify, and delete security associations (SAs) and all respective attributes.

ISAKMP offers a flexible, scalable and standard methodology for distributing cryptographic keys and SAs within high-risk security settings. There are procedures for authenticating peers; creating, generating and managing keys or SAs; and mechanisms to neutralize common network attacks.

Secure Shell (SSH)

Basically, SSH embodies an international standard (comprising several RFCs) that establishes secure logins, channels and transfers between networked devices. It was originally designed to address an administrative need for secure remote login and shell that ensures network privacy to prevent eavesdropping, interception or tampering by a malicious third-party entity.

The primary problem with standard Telnet, FTP and NFS transactions is that they transmit details in plaintext (such as login credentials and exchanged content) that are useful in leveraging an attack. Cryptography naturally suits these purposes (remote login, shell and file copying) and SSH provides the necessary means. SSH version 2 (SSH2) can use traditional username/password logins, public key cryptography and several alternative forms of authentication and continues using service port 22.

Public Key Cryptography Concepts

The underlying concepts of public-key cryptography are known, published, and widely utilized in many security scenarios. It's called *asymmetric* cryptography because separate keys are used for encrypting messages (public key) and decrypting messages (private key), which enables untrusted users to sign and seal a cryptographic message that only the intended recipient may "open".

Public and Private Keys

Asymmetric cryptography introduces the concept of public and private key pairs used for secure exchange of private information across a public network medium. Public and private key construction enables sender and recipient to act as signers of private information (via public key) without having to divulge, expose or reveal any aspect of the decryption (private) key.

Public Key Infrastructure (PKI)

The *public key infrastructure* is a combination of cryptographic algorithms, technologies, protocols, policies and services that enable senders and recipients to securely exchange secrets and confidential information across the public Internet. PKI encapsulates sensitive transactions for transmission across the untrusted public network using a trusted mutual authority—a Certificate Authority (CA), which issues digital certificates for provable identification. PKI consists of the CA issuer, a Registration Authority (RA) verifier, a directory of stored certificates, and a certificate management system.

Registration Authority (RA)

A *registration authority* is tasked with verifying user identities and then instructs the certificate authority to issuing digital certificates. RAs are a core component of the public-key infrastructure, which enables individuals and organizations to security exchange sensitive information. However, an RA is only responsible for authentication and identification of subjects but does not sign or issue digital certificates, which is sole responsibility of the certificate authority.

Certificate Authority (CA)

A *certificate authority* or *certification authority* is any trusted third-party entity that issues digital certificates for use by other parties and are characteristic of PKI cryptography. Commercial CAs charge for services but alternative providers freely issue digital certificates for public consumption. Companies, institutions and governments may implement their own entrusted CAs to sidestep potential exposures, risks and threats associated with external entities.

Certificate Revocation List (CRL)

PKI cryptosystems utilize the *certificate revocation list* to maintain invalidated certificate entries. CRLs are generated and periodically published following a clearly-defined timeframe and can publish immediately following a recent certificate revocation. The CRL is always issued by the CA that issues the corresponding certificates and every CRL contains a valid lifetime (usually 24 hours or less) during which time it may be consulted by a PKI application for verification prior to use.

According to RFC 3280, there are two states of certificate revocation:

- **Revoked:** a certificate is irreversibly revoked if improperly issued, its private key considered compromised, or for lack of adherence to policy requirements (e.g., falsifying documents, misrepresented software behavior, general policy violations).
- **Hold:** a reversible status used to denote temporary invalidity, as in the case of a lost private key; however, should the user relocate that key the certificate status can be revalidated thus removing its entry from future CRLs.

RFC 5280 outlines the ten reasons to revoke a certificate.

Key Registration

Among many likely services to be found in PKI, *key registration* is initially the most important because it handles the issuance of new certificates for public keys. Key registration binds user identities to digital certificates (as produced by the registration authority) for use with certificate authorities. The registration process may be carried out in software (by the CA) or under human supervision.

Key Escrow

Key escrow (also called *key recovery*, *trusted third-party* or the *fair cryptosystem*) arranges for public and private decryption key storage so that an authorized third-party may gain access in circumstances of need. Typically the decryption key to an encrypted communication is kept among only the person(s) directly involved; however, in certain cases a third-party individual (i.e., company or governmental entity) may require possession of decryption keys to investigate an incident or confirm a relationship between parties. A variety of key recovery requirements have been suggested by government agencies conducting covert surveillance within dynamically changing environments encompassing any number of old and new tactics, techniques, and technologies.

Trust Models

The certificate trust model establishes a baseline for entrusting users in a secure exchange. Direct trust is where two communicating parties are responsible for manually verifying signatures. Indirect trust uses a third-party using a CA-issued or self-signed certificate for communication. A hierarchical trust model requires that all party certificates are issued by an independent third-party entity that may issue certificates themselves or certificates used to issue certificates in a chain of subordinates.

PKI based on a hierarchical CA model is composed of well-defined trust and naming standards. Under this arrangement multiple CAs are organized into clearly-defined parent-child relationships. Child CAs are certified by parent CA-issued certificates, which binds a CA public key to its identity. Basic types of CA trust model include:

- **Root trust model:** a CA is either a root or subordinate, and use of offline root CAs provide the highest level of security.
- **Network trust model:** also called *cross-certification*, every CA is both root and subordinate.
- **Hybrid trust model:** combine elements of both rooted and network trust models.

PKI Implementation and Certificate Management

PKI certificate management protocols (like X.509)--defined for all relevant aspects of certificate creation, issuance, and management—help maintain the PKI management model. You must plan all parts of your PKI carefully to avoid subtly compromising or significantly weakening security. For security reasons, the private key used to digitally sign certificates should never be shared with anyone or transmitted across the Internet. Certificates contain the following: name, serial number, expiration date, a copy of the certificate holder's public key and the digital signature of the issuing authority. Some digital certificates conform to the X.509 standard, which is an international standard specifying formats for public-key certificates, certificate revocation lists (CRLs), attribute certificates and certification path validation.

Failure to adequately plan for a secure root CA within a PKI hierarchy could compromise every certificate issued by that CA. Designing PKI to support a single application or process without forward consideration for future requirements can force you to redesign and redeploy, which may also compromise security and availability. Follow industry and organizational best practices for certificate management, enable CRL checking for native-mode clients, and protect the integrity of client authentication certificates. Use certificate trust lists to define the trusted root CAs, use Active Domain in Windows networks to deploy site server signing certificates, and guard that site server's certificate. Use a new key pair when renewing the server certificate and verify that all certificates are kept in secure certificate stores.

Key Escrow

Key escrow systems that must furnish timely law enforcement access to an entire key or plaintext transformation present an unprecedented path to encrypted data recovery. This alternate path is beyond user control and removes a fundamental safeguard against mistaken or fraudulent release of keys or information. Non-recoverable systems can be designed and implemented without any such alternative recovery paths since they're unnecessary for ordinary operation and undesirable in many cases.

Domain 6 - Organizational Security

Organizational computing environments experience a greater intensity, frequency and volume of attack from sources all around the world. Attack methodologies remain the same, but underlying techniques and tactics are born and bred in the undergrounds where blackhats and criminal elements dwell. It's your duty as a Security+ certified professional to identify common threats, typical exposures and identifiable vulnerabilities throughout the organizational landscape.

Concepts and Components to Redundancy Planning

IT security encompasses more than just the obvious security provisions. Nowhere is this more evident than in business continuity planning (BCP) and disaster recovery (DR), two similar though separate aspects of IT security practice. BCP seeks to establish the means, methods and mechanisms through which interrupted business functions are restored to working order.

DR is a complementary strategy that establishes the policies, protocols and procedures necessary to recover disrupted business operations with designated off-site facilities for potential relocation. Common concepts used among both BCP and DR planning follow.

High Availability

Remember that availability—the quality of being accessible when necessary—is a key element in the CIA Triad and a system design protocol that ensures a certain degree of operational continuity. Being available refers to the ability for the user community to freely access a system or service, but *high-availability* denotes a more drastic nature where a business is operating at minimal capacity due to unplanned downtime or unscheduled interruption. Despite disruption to major company operations, critical business functions may persist so that it may limp along until making a full recovery.

Fault Tolerance

What makes high-availability possible is *fault-tolerance*, the quality of resisting and withstanding faults and failures. Fault-tolerance establishes multiple disks in a storage array, redundant public network links, alternate backup sites, and other duplicate trends to ensure that single failure of any component never singularly affects other services, systems, or entire networks. Fault-tolerance is the graceful degradation of service or operation that decreases proportionate to the severity of failure.

Cold Site

A *cold site* a low cost, entry-level backup site solution with the most time-consuming recovery phase of all other options. No original hardware, software or information is carried over until some disruptive event occurs. Lack of setup lowers initial investment cost but incurs additional cost and time penalties stemming from business interruption until recovered and restored to operational condition. Cold sites require very little to no maintenance.

Warm Site

A *warm site* comprises the necessary computing equipment and network connectivity to make a more graceful and timely recovery phase than with cold sites, but with clearly added cost increase. Warm sites may contain incomplete backups (if at all) accounting for business data that is perhaps now days or weeks behind schedule but positioned much closer to the recovery goal line. Any warm site will require a moderate amount of maintenance to keep at operating capacity for sudden transition.

Hot Site

A *hot site* is any backup site location where an interrupted business may continue full operation following a natural disaster or unnatural disruption. Hot sites are specifically defined as being exact duplicates of the original environment, fully operational in every way including near-complete backups of original information. As expected, every hot site requires a heavy amount of maintenance to keep operational including up-to-date changes, mirrored configurations, and recent information.

Backup Generator

Computers, devices and equipment all draw power. Interruption to power is disruptive to service levels built upon these cornerstone infrastructure elements and affects business operations entirely. Having an alternate power source such as a backup generator on-site to run the most business-critical functions is vital to keeping a crippled enterprise limping rather than collapsing helplessly. Emergency power systems provide backup resources in crisis and include deep cycle battery, flywheel energy storage, and hydrogen fuel cell designs.

Single Point of Failure

A *single point of failure* is defined as interruption to any single component that individually (and negatively) affects an entire system. An exemplary situation is where a single router, gateway or public link failure adversely affects an entire network of end-users. High-availability systems (e.g., applications, systems, networks) are often given redundant or doubled-up defenses against these singular failures: doubled network interfaces, storage drives, server configurations, power supplies, etc.

Redundant Array of Independent Disks (RAID)

Availability is an integral part of the CIA Triad and a functional aspect of any secure network environment, right down to the individual systems and storage volumes. *Redundant array of independent disks* enhances the way information is stored and retrieved in high-availability, data-rich computing environments where timely accessibility is strictly required. RAID establishes a multi-disk configuration useful for enhancing I/O performance (striping), data reliability (mirroring), or both (striping and mirroring) at various levels.

Spare Parts

Having *spare parts* or extra hardware on-hand to replace component failures in mission-critical high-availability systems is essential to executing efficient and effective recovery phases. A thorough assessment accounts for all critical components that can reasonably have standby replacements in the event of their total failure. Part of maintaining service level agreements (at the provider level) and high-availability service operation (at the subscriber level) means employing multiple redundant systems and having multiple spare parts to handle multiple potential failures.

Redundant Servers

Redundant servers and redundant services create safety net-like fail-over conditions where primary server or service functions are carried out by alternate secondary servers and services. Redundancy is a pervasive element and permanent fixture of high-availability and assured service level environments where downtime is expressly prohibited. Redundant server and service setups create an operational setting where much-needed resources are constantly accessible because backup and standby units are poised to take over when primary units are taken out. Redundant servers and services also provide *load-balancing* capabilities that distribute large computing or network transactions across multiple servers and services to reduce performance impact and resource utilization.

Redundant Network Connections

A redundant ISP or VPN network configuration continues the same pattern of fail-over safety as redundant servers and services. Critical business transactions require dedicated public leased-lines or other specific arrangements where reliable, sustained connectivity is assured. Every individual line represents a single point of failure; usage of multiple lines (and multiple transmission protocols) increase favorable odds and create multiple points of failure. In some cases, separate Internet connections work in a load-balancing fashion so that when one link's bandwidth becomes saturated (or meets a certain threshold trigger) another accepts overflow traffic to alleviate resource overutilization.

Uninterrupted Power Supply

Some events are unavoidable but most can be prevented or protected against causing serious damage to critical business components. The *uninterrupted power supply* is a universal standby power source that supplies a limited amount of battery backup power when the primary source fails. UPS instantly takes over when the original power source becomes unavailable to provide continuous power to sustain safe and proper computer shutdowns or continue operating a few critical business operations. UPS is a temporary fix meant to service equipment for a finite period until primary power is restored and cannot provide ongoing energy like emergency power systems or backup generators.

Implementing Disaster Recovery (DR) Procedures

Disaster recovery carries the grave implication that some disastrous event has caused disruption or destruction to ongoing business operations. A disaster can be any natural or man-made event ranging from environmental accidents to extreme weather and workplace incidents to acts of terrorism. Either way the end-result is constant: business operations are crippled and impaired in some critical manner.

Disaster Recovery Planning

Planning for DR requires formal assessment of risk, threat and vulnerability specific to a work site, facility and operational nature. DR planning accounts for all the negative consequence that comes from major disruptions to organizational function or operation, including the least-likely remote possibilities. The final product is the disaster recovery plan—a comprehensive statement of consistent actions to be taken before, during, and after a disaster of any origin. This plan must be documented, tested, reviewed, and revised for the duration of its existence. Most importantly, the DR plan must ensure recovery of operations and availability of critical resources in the event of a disaster with the primary objective of protecting the organization in the event that part or all of its operations are halted.

Disaster Recovery Exercises

Few DR plans are static documents that are never exercised or rehearsed. DR is a trend-following live document format that adapts to changing circumstantial, environmental, or surrounding conditions. DR rehearsal exercises the mechanisms, methods, and manpower that facilitate recovery procedures. *Pilot testing* is the practice of validating application updates, configuration changes, and system modifications prior to deployment. Perhaps nowhere is this more necessary than in proving the correctness of DR strategies.

Backup Techniques and Recovery Schemes

The best recovery strategy for disruptions and disaster is creating current, consistent backups. The best recovery strategy is specific to the conditions, considerations and criteria for a given site or situation. It can be simple (e.g., Tape, USB, CD, DVD) or complex (e.g., offsite, mirroring, encrypted) to suit a variety of needs, but every backup process must be repeated and consistent.

Backup methods are summarized in the following:

- **Full backup:** the starting point for all other types; contains a complete set of data representing the folders and files selected for duplication. Restores all files and folders and results in faster and simpler restore operations but may be inefficient in terms of processing overhead.
- **Differential backup:** contains only files that have changed since the last full backup and considerably shortens backup and restore periods. Overdoing differential backups can cause backup image size to grow beyond the baseline full backup image.
- **Incremental backup:** stores all files changed since the last full, differential or incremental backup procedure. Completes in less time than other methods but individually processes incremental backup images during restoration, which can elongate recovery times.
- **Mirror backup:** similar to full backup but typically without file compression, encryption or password protections offered by commercial solutions. Mirror backups are exact duplicates of original on-disk data.

Data backups can also be created using online services but there are overhead and security implications to thoroughly consider. Offsite data backups also present unique advantages and disadvantages that must be specially considered for each site and situation.

Recovery and Restoration

BCP and DR strategies are defined by recovery and restoration procedures, two concepts that are closely related but lead mutually separate existences. *Recovery* basically describes the return to an original state or the act of regaining something lost—in a computing context, this carries the implication of a serious disaster or disruption to communications, services or operations. *Restoration* is also similarly defined as bringing something back to its original condition, existence, or state—but in a computing context, the implication of disastrous failure is absent. Hence the separate branches of business continuity and disaster recovery planning.

Using those concepts, business continuity restores functionality or operations impaired or interrupted by some temporary condition or non-terminal event. Disaster recovery is the process of restoring functionality or operation disabled or disrupted as a result of long-term power outage, natural-born destruction, environmental accident, fire damage, or other enduring situation.

Incident Response Procedures

Medium to large organizations typically maintain incident response teams consisting of several key players from major departments. An ideal emergency and incident response team comprises several members including: security specialists, IT professionals, legal representatives, management contacts, and a public relations member. The basic premise of incident handling and incident response is that a company requires a clear plant of action with designated roles detailing each member's respective expectations and responsibilities.

Incident response teams accomplish the following tasks:

- **Initial assessment:** Determine whether it is a false positive (one of the two types of a false alarm). Determine whether the attack is still in progress. Do some preliminary research as to what type of attack the organization is dealing with and what the potential damage areas and severity are.
- **Initial communication:** Personnel assigned to the alarm, if suspecting a real incident, should notify the appropriate people as soon as possible.
- **Initial containment of the incident:** Set priorities and follow them closely. They vary depending on the organization, but the list usually begins with protection of classified data, then business and proprietary data, and then actual systems (be it hardware or software). The key question is, "Do I pull the plug?" The security response team has to be clear about what to do.
- **Intrusion evaluation:** Determine the origin of the attack, its purpose, the type of attack, the tools and mechanisms used, and the systems and files that were accessed successfully or unsuccessfully.
- **Forensic evidence collection:** Actions from the plan category are likely to yield some meaningful results. The next action plan item is gathering all the information learned about the incident up to this moment.
- **Communication of the incident in public:** In contrast to the initial communication (the purpose of which is to bring the problem to the attention of the right people within the company), public communications can be subdivided into several categories.
- **Service restoration:** Next, the incident response team needs to evaluate whether the systems should be repaired, restored, or completely rebuilt.
- **Incident report preparation:** Contrary to public communication, this report is an internal document that puts everything in perspective from the minute te incident was noticed.

At any point during the incident response process one or several members may also perform extensive duties as outlined in the following paragraphs.

Digital Forensics

Digital forensics (also *computer forensics*) is a specific branch pertaining to acquiring, intercepting or seizing legal evidence contained within computers, electronics, and digital storage mediums. Computer forensics searches *digital artifacts* (e.g., disk drives, ROM discs, electronic documents, image formats) or even packet sequences in network traffic. The objective is to explain the current state of those digital artifacts as evidence in a criminal investigation. Obviously there are certain industry and legal restrictions, requirements and regulations enforced when using digital information as evidence in pursuit of a criminal conviction.

Chain of Custody

Among the more crucial aspects of securing evidence of any nature is the *chain of custody* or chronological history documenting its capture, custody and control. Analysis, disposition, and transfer of evidence (both digital and physical) must be conducted in a careful, scrupulous manner to avoid allegations of tampering, tainting, or compromising misconduct. Even the slightest discrepancy in the chronological events describing the nature of evidence is sufficient grounds for compromise.

First Responders

As outlined in every BCP and DR strategy and practiced in virtually every corporate computing environment, *first responders* are the initial crash and crime scene investigators that lead the initiative toward controlling, investigating or managing a critical circumstance, disruption or event. They are designated point men and point women who arrive to kickstart cleanup, restoration and recovery processes, and facilitate damage control procedures.

Damage and Loss Control

Damage control and *loss control* refer to identical processes of preventing further destruction to company assets or disruption to company resources. It's the effort to curtail damage and minimize loss and regain control of an out-of-control situation. Damage/loss control procedures are developed according to site-specific conditions and circumstances, which vary according to regional, environmental and territorial threats.

Reporting and Disclosures

For every publicly-held company is a publicly-accountable labor force responsible for disclosing earnings and successes or reporting losses and failures. Governmental agencies, financial organizations, and healthcare institutions are responsible for disclosing attacks, exposures, and thefts related to personally identifiable information. Electronic commerce and online payment systems are responsible for reporting compromises to account holder information. Certain industries are held to revealing particular crimes as they affect clients, customers, or consumers in very specific ways as governed by federal mandates, governmental laws, and industry regulations.

Legislative and Organizational Policy

Company security policy objectives are derived from several key sources including governmental legislature, federal regulations, industry practices, and organization-specific considerations. Other non-mainstream sources also indirectly contribute to policy development but none are more pervasive and persuasive than the laws and mandates imposed by federal or governmental bodies, which often demand proven compliance under penalty of law. These two primary sources often direct organizations in handling patient records (healthcare), credit information (e-commerce), personal information (state agencies), or other processes related to securing confidential data and functions.

A handful of the various individual security policies include the following:

- **Acceptable Use Policy (AUP):** defines company-sanctioned accepted usage trends for an organization's physical resources and intellectual properties.
- **Audit Policy:** defines requirements and parameters for risk assessment and audits of the organization and information resources.
- **Extranet Policy:** establishes requirements for third-party entities desiring remote access to internal company resources.

- **Password Policy:** outlines the benchmarks and standards by which password security is gaged and measured, including guidelines for password selection best practices.
- **Wireless Standards Policy:** details conditions and criteria for accepted wireless device connectivity and preventive safeguards against wireless intrusions.

Other related topics follow in subsequent paragraphs.

Secure Disposal of Computers

Disposing of sensitive information is a delicate issue—both in terms of application and consequence. It appears that some companies and organizations fail to properly sanitize sensitive information (electronically and mechanically) prior to disposal, which has led to several high-profile cases of sensitive information being exposed to unauthorized sources. Resold mobile phones, media players, and removable media have revealed secret military and governmental information; repurposed corporate computers have revealed active security keys and login factors; and reused flash storage devices often leave recoverable data even after storing new data. Secure computer disposal requires the appropriate level of destruction to match the level of confidentiality or secrecy involved, which may including several encrypted passes the full capacity of a storage volume to total hard drive incineration.

Acceptable Use Policy (AUP)

An *acceptable use policy* outlines absolute conditions, behavioral expectations, and enforced rules for a given computer system or network—as defined by administrators, security professionals, and legal experts. AUP is written for business, corporations, institutions, providers, and universities to reduce the potential for legal action taken by a user and legal conditions applicable to end-user interactions. AUP is often used to establish explicit end-user acceptance or denial of AUP terms prior to granting (or rejecting) access to protected resources and systems. Documented policy often mirrors Terms of Service conditions specified by email and Internet service providers.

Password Complexity Enforcement

The strength of a password is a function of its complexity, length, and randomness. Even the strongest encryption algorithm from the best cryptographic implementation cannot protect against poor end-user password choices—and those choices are vast and varied. An established password complexity security policy augmented by digital, electronic, and mechanical enforcement ensures that users make appropriately challenging password choices every time. Enforcements against derivative username passwords (joe/joe123), dictionary words (spelled forward and backward), short lengths, and non-varied character composition (i.e., only letters or numbers) provide the greatest initial strength for your security policy strategy.

Change Management

Change management is an IT service management discipline with the sole objective of ensuring that standardized methods and procedures establish sufficient management, monitoring, and reporting of changes to a controlled IT infrastructure. Change management tracks alterations to the IT infrastructure that may arise reactively or responsively due to externally-imposed requirements (e.g., legislative, regulatory or industrial changes) or from internally-imposed initiatives (e.g., efficiency enhancement, security improvement, implementation upgrade). The process of managing change ensures that standardized methods, processes, and procedures are used to facilitate efficient, prompt handling of change while striking balance between change and consequence.

Information Classification

Information classification restricts access to protected information as restricted by law or regulation to particular classes of personnel. Formal security clearances are required to access and handle classified information, which is categorized into a series of security labels defining their secretive nature (e.g., Secret, Top Secret, or Classified). Some corporations and non-governmental organizations also assign sensitive information in compartments of access to prevent foreign dissemination to US nationals and originator-controlled dissemination enabling the tracking of sensitive information.

Mandatory Vacations

Employees operating in sensitive areas of the business should be forced to take vacations in what is known as a *mandatory vacation* policy. In their absence, other individuals fulfill their roles and responsibilities and are capable of detecting fraudulent behavior, inappropriate activity, or erroneous results. Any problems specifically related to the original employee's accounts or activities will be noticeable in their absence—either a previously unknown problem will be discovered or an existing problem may temporarily cease.

Personally Identifiable Information (PII)

Generically defined *personally identifiable information* is a class of data pertaining to the contact, location or identification of specific individuals. The NIST *Guide to protecting the Confidentiality of Personally Identifiable Information* specifically describes PII accordingly:

> *Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.*

PII is currently a hot topic because of many high-profile data thefts and information attacks supportive of identity theft rings and crimes against business clients and consumers. Stored PII falls under several federal, governmental and industrial regulations that dictate how confidential data is stored, transmitted and ultimately destroyed—all depending upon the nature of business and sensitivity of information.

Due Care

Simply defined, *due care* means knowing and performing the proper course of action in every situation and taking responsibility for those actions. Due care is the action, behavior, or character expected of a reasonably prudent person to act upon, regardless of the individual's security function or occupational role. Due care also defines the steps taken by a company to prove responsibilities for actions taken during the organization's daily routines and business operations. A business exercises due care by implementing policies, procedures, and processes to protect its assets, personnel, and resources.

Due Diligence

Due diligence in a computer security context is part of the information technology procurement process to ensure risks are known, threats are managed, vulnerabilities are protected and exposures are safeguarded from attack. During mergers and acquisitions, due diligence reviews identify and assess business risks associated with acquiring, integrating and operating separate business components.

Due Process

Due process is the principle that a person has the right to be notified and heard in an orderly proceeding to protect that individual's rights. In doing so, a person is assured fairness, liberty, and justice in pursuing some legal matters. Simply stated, due process describes the course taken during court proceedings to safeguard legal rights of individuals.

Service Level Agreement (SLA)

A *service level agreement* contractually guarantees an agreed-upon level of service between provider and subscriber. Contractual obligations are expressly between subscriber and provider—no third-party reseller or entity may enter such agreements or guarantee such service levels. Each area of service has defined "level of service" scopes specifying levels of availability, serviceability, performance, operation or other attributes. Levels of service may be specified as measurable average "target" or lowest expectation "minimum" service level terms. This practice once described fixed-line telecom operations but sees widespread usage across a broad spectrum encompassing all industries and markets.

Human Resources (HR) Policy

The *human resources* section of company security policy specifies the proper handling of personnel throughout the pre-employment to post-employment cycle, particularly with respect to its affect on organizational security. HR policy can get highly detailed but minimally covers entire employment lifecycles while addressing the different security concerns associated with each phase.

It is critical to establish a security policy that covers hiring practices such as background checks, follow-up on references, educational records verification, and ensuring that staffers sign-off on various HR-related documentation (e.g., employment agreements, non-disclosure agreements, security policies, business ethics, usage agreements). Organizations incur liability where no policy exists (or no procedure to enforce compliance) that specifically covers the full and timely removal of privilege and rights of terminated individuals who then cause resultant damage, destruction, or disruption.

User Education and Awareness Training

A major factor in the HR policy lifecycle is user education and awareness training—strict advisory, guidance, and learning programs aimed at instructing and informing end-users on company security policy. Users encompass all manner of technical and non-technical personnel comprising varying levels of threat awareness, secure computing know-how, and risk avoidance practices. Every employee needs to be informed of company security policy, which changes by occupation and organization. Companies need formal educational and training regimens to inform its employees of site-specific threats and associative vulnerabilities. End-users are typically among the weakest links in any organizational security chain, rivaled only by bad security practices.

Environmental Security Controls

A damaged or destroyed working environment is an unsecured working environment. Imagine receiving significant structural damage to a building that exposes sensitive server hardware and workstation computers. Securing those items becomes increasingly problematic with regard to the nature and intensity of damage sustained—it's not like you can rebuild insulated brick walls overnight or repair structural damage with tools on hand. Fire, electricity, gase, water, and natural elements continually conspire to damage the working environment and disrupt security.

Fire Suppression

A proper *fire suppression* system seeks to slow or halt the spread of a fiery outbreak. Many chemical, liquid, and other types of suppression system exist to address the various particulars and needs of a , given environment. Certain high-value computing assets may be protected by alternative suppression systems that reduce further incidental damage (i.e., water damage) in the process of extinguishing flames or fluctuating temperatures.

Heating, Ventilation and Air Conditioning (HVAC)

Ideal environmental conditions collectively preserve the delicate hardware and sensitive instrumentation used to secure and maintain the business infrastructure. High-heat, excess humidity, water damage, turbulent winds, and violent thunderstorms can adversely affect the enterprise landscape in a multitude of ways. Design considerations for HVAC include: independent power source, positive air pressure (i.e., air constantly flows out to avoid inbound contamination), protected intake vents to prevent intrusions or tampering, monitoring of environmental conditions, emergency cut-off, and secure placement of the HVAC system.

Shielding

Shielding sensitive equipment from errant emanations and environmental interference is instrumental to maintaining an orderly, secure computing environment. Shielded cabling, such as coaxial, safely encapsulates a copper core in layers of protective sheathing materials. This prevents intentional damage during installation and usage, and also serves as an indicator to intrusive splicing. Shielded monitors prevent sensitive emanations from being observed by passive parties, who may watch undetected over a sensitive end-user session.

Trickery, Thievery and Social Attacks

Not all computer-related attacks are high-tech; some even make minimal or no use of technology. A good security practitioner is a keen observer of his or her surroundings and maintains good situational awareness—because attacks can come from any angle in just about any form. It could be a phone call, an email, or just some casual (but nosy) bystander. Security+ examination covers basic non-technical attacks against all types of people from all kinds of sources, some of which are covered below.

Social Engineering

Information security defines *social engineering* as the act of manipulating people into divulging sensitive information or performing authorized acts for some unauthorized third-party entity. Most victims of social engineering attacks never personally encounter their attackers but are compelled to reveal confidential or personal information. Social engineering targets specific short-circuit decision-making biases in human thinking that lend to faulty behavior. Social engineering attacks range from email messages requesting login credentials, text messages requesting account holder information, phone calls from an assumed authority figure, or baiting victims through other means.

Phishing

The criminally fraudulent process of obtaining personal information directly from the source while masquerading as a trustworthy entity (e.g,. on-duty manager, system administrator, loan officer). User credentials, credit details, financial information, and other PII are frequently the valued gains that fraudsters are seeking. Phishing takes many forms email spam to instant messages and even mobile phone texts.Increasingly convincing fake Web sites are a most popular redirection where phishers attempt to obtain online banking login information to pursue account thefts and other financially ruining criminal activities.

Internet Hoaxes

An *Internet hoax* is simply a low-tech attack predating upon the collective general naiveté or technological ignorance of its target audience. The hoax is an attempt to dupe or deceive its audience into accepting, believing or conceiving that a falsehood is real and true. Classic Internet hoax format follows traditional urban legends but are generally reworked or written in a computing context and use e-mail or web sites as a vehicle. Internet hoaxes are essentially practical jokes intended to mislead its readers with no ill effect, but in some cases the wrong hoax at the right time can have consequence—such as announcing false reports of financial or internal troubles to drop a company's stock value.

Shoulder Surfing

Shoulder surfing is another low-tech attack that's really a basic invasion of privacy by nosy busybodies and unscrupulous individuals overlooking your computing activities. An observer may be posted around or behind you in a cubicle setting, standing within sight of your ATM transaction, or stationed within range of binoculars but the overall end-result remains identical. Truly effective shoulder surfing attacks are difficult for the victim to detect because they're preoccupied by some activity (e.g., inputting a PIN, typing a password, pressing a numeric keypad) that engages their full attention—and the attacker's.

Dumpster Diving

Classic *dumpster diving* (also called *trashing*) is the practice of sifting through garbage to recover discarded items of value to the dumpster diver. In a computing context, dumpster diving is the invasive act of rifling through waste bins to discover confidential, proprietary or sensitive information carelessly discarded without consideration to its value. The dumpster diver varies in sophistication and targets whatever information suits: financial data related to acquisitions and mergers; employee payroll information; credit card details; social security numbers; and any other manner of private data.