

(ISC)²[®]

SSCP



**Smarter
Training**

This LearnSmart exam manual covers the most important topics and objectives you will encounter on the Systems Security Practitioner exam (SSCP). By studying this manual, you will gain familiarity with an array of exam-related content, including:

- Access Control
- Administration
- Audit and Monitoring
- Cryptography
- And more!

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

SSCP® LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC
Product ID: 010661
Production Date: July 19, 2011
Total Questions: 25

All rights reserved. No part of this document shall be stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

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.

LearnSmart Cloud Classroom, LearnSmart Video Training, Printables, Lecture Series, Quiz Me Series, Awdeeo, PrepLogic and other PrepLogic logos are trademarks or registered trademarks of PrepLogic, LLC. All other trademarks not owned by PrepLogic that appear in the software or on the Web Site (s) are the property of their respective owners.

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

Abstract

This Exam Manual reviews the major topics and perspective points for the SSCP® exam from ISC2. This manual is divided up into seven primary sections which correspond to the seven domains of the SSCP® exam: access controls; administration; audit and monitoring; risk, response and recovery; cryptography; data communications; and malicious code. This manual is designed to serve several purposes. First, it can be an introduction to the broad range of topics covered in the SSCP® exam. Second, it can serve as a guideline to pursue more in-depth study and research using other resources. Third, it can be used as a litmus test to see how much information you already know or have obtained through study. Fourth, once you are familiar with each topic on this Exam Manual, you should be adequately prepared to take the SSCP® exam.

What to Know

Any area or topic that you are not already thoroughly familiar with should be the focus of your own personal exploration, research and study. Reference materials as well as the Internet are usually excellent resources to pursue further depth or obtain different perspectives on the SSCP® exam topics. This manual is not 100% exhaustive, but rather is a manual, an overview, and a list of the most common and most significant issues and topics. Using this manual alone is probably not sufficient, but using it in combination with other resources (online, print, and practice questions), should greatly improve your chances for success on the SSCP® exam.

Tips

Take as many practice questions as you can. You should also take the effort to read and research in depth on each and every topic that you are not thoroughly familiar with. This may include the purchase of exam preparation books, scouring of the Internet, or working through practice exams. The more effort you put into absorbing, understanding, and even applying the knowledge associated with SSCP®, the better your chances become at passing the SSCP® exam itself.

Table of Contents

Abstract	3
What to Know	3
Tips	3
Access Controls.....	11
Accountability.....	11
Identification and Authentication Techniques	11
Knowledge-based	12
<i>Token-based</i>	12
<i>Characteristic-based</i>	13
Tickets (Kerberos)	13
One-Time Passwords (OPIE)	13
Single Sign On (SSO).....	14
Password Administration	14
<i>Selection</i>	14
<i>Management and Control</i>	15
Access Control Techniques	15
<i>Discretionary Access Control</i>	15
<i>Mandatory Access Control</i>	15
<i>Access Control Lists</i>	15
<i>Principle of Least Privilege</i>	15
<i>Segregation of Duties and Responsibilities</i>	16
Account Administration	16
<i>Account, Log and Journal Monitoring</i>	16
<i>Access Rights and Permissions</i>	16
Access Control Models, Methodologies and Implementation	17
File and Data Owners, Custodians and Users	17
Methods of Attack	17
<i>Brute Force</i>	17
<i>Password hashes</i>	18
<i>Denial of Service</i>	18
<i>Dictionary</i>	18
<i>Spoofing</i>	19
<i>Man-in-the-middle attacks</i>	19

<i>Spamming</i>	20
<i>Sniffers</i>	20
<i>Crackers</i>	20
<i>Monitoring</i>	21
<i>Intrusion Detection</i>	21
<i>Alarms and Signals</i>	21
<i>Audit Trails</i>	21
<i>Violation Reports</i>	22
<i>Penetration Testing</i>	22
Administration	23
Security Administration Principles.....	23
<i>Privacy</i>	23
<i>Confidentiality</i>	23
<i>Integrity</i>	24
<i>Availability</i>	24
<i>Authorization</i>	24
<i>Identification and Authentication</i>	24
<i>Accountability</i>	24
<i>Non-repudiation</i>	24
<i>Data Classification</i>	25
<i>Documentation</i>	25
<i>Audit</i>	25
Security Architecture.....	26
<i>Design objectives</i>	26
<i>Development life cycle</i>	26
<i>Security control architecture</i>	26
Protection mechanisms.....	27
<i>Layering and Data Hiding</i>	27
<i>Abstraction</i>	27
<i>Modes of operation</i>	27
<i>Data/information storage</i>	27
<i>Configuration Management</i>	28
<i>Data Classification</i>	28
<i>Information/Data Collection and analysis techniques</i>	28

<i>Employment Policies and Practices</i>	29
<i>Policies, Standards, Guidelines and Procedures</i>	29
<i>Roles and Responsibilities</i>	29
<i>Security Awareness Training</i>	30
<i>Security Management Planning</i>	30
<i>Data/Information System Attacks</i>	30
<i>Interrupts</i>	31
<i>Remote maintenance</i>	31
<i>Logic bomb</i>	31
<i>Trap door</i>	31
<i>Browsing</i>	31
<i>Spoofing</i>	31
<i>Exhaustive</i>	31
<i>Inference</i>	32
<i>Traffic analysis</i>	32
<i>TOC/TOU</i>	32
Audit and Monitoring	32
Control types.....	32
<i>Security Auditing</i>	32
Monitoring tools and techniques.....	33
<i>Warning banners</i>	33
<i>Keystroke monitoring</i>	33
<i>Traffic/trend analysis</i>	33
<i>Event monitoring</i>	34
<i>Real-time</i>	34
<i>Closed Circuit Television (CCTV)</i>	34
<i>Intrusion detection</i>	34
<i>Illegal software monitoring</i>	34
<i>War dialing</i>	35
<i>Sniffing</i>	35
<i>Eavesdropping</i>	35
<i>Radiation monitoring</i>	35
<i>Dumpster diving</i>	35
<i>Social engineering</i>	35

<i>Inappropriate activities</i>	35
<i>Fraud</i>	36
<i>Collusion</i>	36
Cryptography	36
Cryptographic concepts, methodologies, and practices	37
<i>Symmetric vs. Asymmetric</i>	37
<i>Symmetric Key Cryptography</i>	38
<i>Asymmetric Key Cryptography</i>	38
<i>Message authentication</i>	38
<i>Digital signatures</i>	38
<i>The basic functionality of hash/crypto algorithms</i> <i>(DES, RSA, SHA, MD5, HMAC, DSA), and effects of key length</i>	39
<i>Key length and security impact</i>	40
<i>Key management</i>	40
<i>Key distribution methods and algorithms</i>	40
<i>Error detecting features</i>	41
<i>Key escrow and key recovery</i>	41
<i>Vulnerabilities to cryptographic functions:</i>	41
<i>Attack methods</i>	41
<i>Certificate Authorities (CAs) and Public Key Infrastructure (PKI)</i>	42
<i>Classification Criteria</i>	43
<i>Secure Protocols</i>	44
<i>The application of hardware components, such as smart cards, tokens</i>	44
<i>IPSEC</i>	45
Data Communications	46
<i>Physical Layer</i>	47
<i>Data Link Layer</i>	47
<i>Network Layer</i>	47
<i>Transport Layer</i>	47
<i>Session Layer</i>	47
<i>Presentation Layer</i>	47
<i>Application</i>	47
<i>Network Topologies (e.g., Star/Bus/Ring)</i>	49
<i>TCP/IP Protocol Characteristics and Vulnerabilities</i>	49

Local Area Networks (LANs)	50
Wide Area Networks (WANs).....	50
Remote Access/Telecommuting Techniques	50
Internet/Intranet/Extranet.....	50
Firewalls	51
Routers.....	51
Switches	51
Gateways	51
Proxies	51
Protocols.....	52
Transmission Control Protocol/Internet Protocol (TCP/IP).....	52
Network Layer Security Protocols (IPSEC, SKIP, SWIPE)	52
Application Layer Security Protocols	52
CHAP and PAP.....	53
Tunneling	53
Virtual Private Network (VPN)	54
Network Monitors and Packet Sniffers	54
Network Address Translation (NAT)	54
E-mail security	54
Network Attacks and Countermeasures.....	55
ARP	55
Brute force	55
Worms	56
Flooding	56
Eavesdropping	56
Sniffers.....	56
Spamming.....	57
Malicious Code	58
Malicious code concepts.....	58
Definitions	58
Behaviors	59
Jargon	59
Myths/hoaxes	59
Hackers, crackers, phreaks, and virus writers.....	59

<i>Denial of service</i>	59
<i>Computer viruses and other forms of malicious code</i>	60
<i>Various types of computer viruses</i>	60
<i>Worms</i>	60
<i>Trojan horses</i>	61
<i>Logic bombs</i>	61
<i>Salami attack</i>	61
<i>ActiveX</i>	61
<i>Java</i>	61
<i>Mobile code</i>	62
<i>Trap doors</i>	62
How malicious code can be introduced into the computing environment	62
<i>Brute force</i>	62
<i>Dictionary attacks</i>	63
<i>Spoofing</i>	63
<i>Pseudo flaw</i>	63
<i>Alteration of authorized code</i>	63
<i>Flooding</i>	63
<i>Spamming</i>	64
<i>Cramming</i>	64
<i>ActiveX</i>	64
<i>Java</i>	64
<i>Mobile code</i>	64
<i>Trap doors</i>	64
<i>Anti-viral protection</i>	65
<i>Loading software only from trusted sources</i>	65
<i>Making frequent backups</i>	65
<i>Installing change detection software (integrity checker)</i>	66
<i>Implement a user awareness program</i>	66
Risk, Response, and Recovery	66
Risk Management	66
<i>Risk management tools and methodologies</i>	66
<i>The principles of risk management</i>	66
<i>Risk Management Process</i>	67

<i>Risk reduction/assignment/acceptance</i>	67
<i>Incident Handling and Investigations</i>	67
<i>Security incidents</i>	68
<i>Incident response</i>	68
<i>Investigations</i>	68
Business Continuity Planning and Disaster Recovery.....	68
<i>Business continuity planning process</i>	69
<i>Disaster recovery planning process</i>	69
<i>Response Teams</i>	69
<i>Plan Testing</i>	70
Practice Questions	71
Answers and Explanations	77

Access Controls

Access controls are used to define and control the actions that users can perform within a secured environment. This includes what systems they can use, what resources they can access and what type of interaction they are allowed to perform with those assets. Access controls enforce the concept of authorization. Access controls include both security mechanisms and theoretical concepts. As an SSCP® candidate, you need to be familiar with both the implementation of these mechanisms, as well as the theory behind them and why they are employed.

Accountability

Accountability is the security concept of being able to hold a human responsible for their actions, whether they are performed in the physical world or within the digital world via a user account. In order to support accountability, an environment must enforce strong authentication techniques, strictly impose the principle of least privilege, monitor every aspect of the environment and perform rigorous inspection of the resulting audit logs.

True accountability will allow the information security officers to be aware of every logon event by every valid and invalid user, every activity each and every user account attempted to perform, and the results of those actions. Accountability is not only knowing what did and did not occur; it also must include job action warnings, punishments and criminal investigations when necessary.

Identification and Authentication Techniques

Identification is the process of claiming an identity for the purposes of gaining access to a secured environment by representing yourself as a valid participant. Identification is usually integrated with, and immediately followed by, authentication. **Authentication** is the process of proving the claimed identity. The act of providing proof is designed to establish that a given user is *the* human operator assigned the responsibility for, and privileges over, the physical environment or the digital entity known as the user account. When strong authentication is enforced, only authorized humans can ever gain entry into a secured environment using an authorized user account.

Identification is a one step process where a single authentication factor (see below) is used to claim an identity. Once the user has claimed an identity, they must then provide proof that they are the authorized individual who can either enter into the physical structure or can control the secured user account.

Authentication can be a single-step or multi-step process. In most cases, a multi-factor authentication is stronger than a single-factor authentication. There are three generally recognized authentication factors:

- Type 1: **something you know** (a.k.a. knowledge based factor)
 - Items of knowledge that you have memorized and can repeat verbally or on a keyboard when necessary. Common examples include passwords, PINs, pass phrases, ID numbers, user names and codes.
- Type 2: **something you have** (a.k.a. token based factor)
 - Physical devices that you are in possession of. They are used as a storage device or a computational device for the authentication process. Common examples include smart cards, token devices, and USB flash drives.

- Type 3: **something you are** (a.k.a. characteristic based factor)
 - Aspects of your human body; this is commonly referred to as biometrics. Common examples include fingerprints, hand prints, facial recognition, voice recognition, iris patterns, retina patterns and keystroke dynamics (how you use the keyboard).

When using authentication factors, any single factor is considered weak in comparison with multiple different factors. Notice the specification that the factors must be different; this is because multiples of the same factors can be compromised by the same act of authentication cracking. Thus, by employing two or more different authentication factors, multiple successful authentication cracking attacks must be successful at the same time, without being detected, in order to grant the intruder access to the secured environment.

Two-factor authentication always means two different factors are used together. Multi-factor, or strong authentication, can mean two or more of the same factors, or two or more different factors. Thus, some forms of multi/strong authentication are weaker than two-factor, and vice versa.

Knowledge-based

Knowledge based authentication factors are strings of characters and/or words that you must reproduce exactly when attempting to authenticate. The most common examples are passwords, PINs and pass phrases. But ID numbers, user names and codes are also valid examples.

Knowledge based authentication factors are improved by making them longer, using many different character types, changing them often and not repeating them (either on other systems or on the same system in the future). Knowledge based authentication factors, once defined by a user, should never be revealed to other people. Furthermore, knowledge based authentication factors should never be written down or electronically stored in a manner that can be easily discovered and stolen by anyone.

Token-based

Token based authentication factors are devices that users must be in physical possession of at the time of an attempted logon or entry. Each token device is tied to the human/user so that if the wrong device is used, or a non-device logon is attempted, access is denied. Common examples include smart cards, token devices and USB flash drives. Token based authentication factors are rarely used as a single factor, since the token can be used by anyone, without impunity, if it is stolen. Instead, token based authentication factors often require a type 1 factor (password or PIN) to use the device. Thus, most token based authentication systems are two-factor by default.

Smart cards or key cards can store hashed passwords, private-keys from a PKI system or digital certificates issued by a certificate authority.

Token devices are available in several forms, including static, symmetric and asymmetric. A static token device simply stores a password. Such a device is often insecure because it usually "protects" stored passwords with a weak, static password. A symmetric token device creates one-time passwords based upon time intervals and a unique algorithm tied to the user account. An asymmetric token device (a.k.a. a challenge response token device) produces one-time passwords based on a challenge-response dialog between the authentication server and the client system. These later two forms of token devices are secure. However, if the device's battery expires, then they must be re-configured using an administrator account which is superior to the account to which they are tied. Thus, token devices cannot be used on the most powerful accounts, such as the root or default administrator accounts.

USB flash drives can serve as a versatile form of smart card and token device hybrid.

Characteristic-based

Characteristic based authentication factors use a biometric (a feature of the human body) or a behavior (an activity or function of the human body) as proof of identity. Common examples include fingerprints, hand prints, facial recognition, voice recognition, iris patterns, retina patterns and keystroke dynamics. Characteristic based devices are worth considering as additional authentication factors, but as with short passwords, they should not be used alone. While biometrics sound high-tech and futuristic, they are still human created technology, and therefore not perfect. Every form of authentication can be fooled given enough time, effort and resource. So, don't rely upon any single factor for authentication, including biometrics, and especially in sensitive environments.

Tickets (Kerberos)

Ticket based systems often perform their operations transparently to the users of the environment. In a ticket based system, authorized members of a realm or domain are issued proof of their membership in the form of electronic tickets. These tickets serve as their identity proof from that moment forward, until the ticket expires. When a ticket is encountered, the receiver checks the tickets timestamp and the issuing authority, if they are current and known, then the ticket is accepted (i.e. the identity of the other entity is accepted). Ticket based systems are often called trusted-third party authentication systems.

The most well known ticket based system is Kerberos. Kerberos uses two types of tickets: Ticket Granting Ticket (TGT) and Service or Session Ticket (ST). The TGT is issued to all valid members of the Kerberos realm after they have proven their identity to the master of the realm (i.e. the KDC or key distribution center). Once a member of the realm (a.k.a. a principle) with a valid and current TGT, they can request permission to interact with other principles via the KDC. If approval is granted the ST is issued to the requesting principle. This ST is then transmitted to the target principle to request interaction with its resources. If the target is able to verify that the ST is valid and the related TGT is valid, it will allow communications to take place. Think of TGTs as passports *into* the realm and STs as the plane or bus tickets used to get *around* the realm.

One-Time Passwords (OPIE)

A one-time password (OTP) is a password that can be attempted only once before it becomes invalid or expires. That means that if the current password is typed incorrectly, then that password becomes invalid. Users only get one chance to type in a one-time password correctly; otherwise the next valid password must be obtained and used. One-time passwords cannot be implemented as a Type 1 factor; instead, they are implemented as a Type 2 factor. When used properly, one-time passwords are the most secure form of password possible. However, the one-time password concept is based on the idea of randomly generated passwords. Since computers cannot produce true random numbers, one-time passwords are not truly random either. Thus, modern implementations of one-time password solutions are actually pseudo-one-time passwords. They remain very strong and reliable, but they are not perfectly strong and reliable.

OPIE, or One-time Passwords In Everything, is a UNIX/LINUX add-on kit that will replace many existing insecure daemons and services with versions that support OTP. It also includes modules that allow customization and addition into other non-standard client and server systems.

Single Sign On (SSO)

Single sign-on is the concept of being able to authenticate into an environment once, then be able to roam about the whole environment without being required to re-authenticate at each new server encountered. This is a common element of most modern client/server networks, especially those based around a directory service or LDAP solution. Single sign-on is the opposite of requiring users to log into each and every server on a network separately, often with a different and unique username and password (and/or other authentication factor). Single sign-on is more of a convenience issue than security issue. With single sign-on, users only need a single set of authentication factors, which can be stronger than what would occur if multiple sets were required. Also, administrators only need to manage a single master database of accounts, rather than separate authentication databases on each server. As long as the single authentication is strong and reasonable and authorization controls are enforced, SSO is a reasonable solution. However, some highly sensitive and secure environments are reverting back to pre-SSO solutions in order to reduce the likelihood that a single user account intrusion could compromise the entire networked environment.

Password Administration

Password administration is the collection of tasks required to maintain a reasonably secure, password-based authentication system. This involves three primary tactics: selection, management and control.

Selection

When users select passwords, they need to do so under the guidance of company security policy. This policy should include awareness training that equips users with the ability to pick strong but memorable passwords. As a general rule of thumb, longer passwords are better than shorter ones (see Brute Force section). It is better to pick a 20 character password comprised of four simple 5 letter words, than an 8 character password comprised of numbers and symbols. The latter may look more complicated, but the former is actually stronger based on the way passwords are stored and used.

Passwords are hashed before being stored in an accounts database and transmitted (at least in modern secure environments). Once hashed, the construction parameters of the original password are completely unknown and undiscoverable to anyone but the original user. All passwords on all user accounts within a single system produce a hash that is of the same length. Brute force attacks can break short passwords quickly, but each time you add a single character to the length of the password, you make the password 130 to 255 times stronger. Thus, long, simple passwords are better than short, complex ones.

Passwords should never be just one or two words. A user should always use 4 words or more. Don't use words that are commonly found together or related. For example, don't pick a line from a movie, song or poem. Don't pick words from the same conceptual arena, such as education, industry, hobbies, interests, experiences, possessions, children, etc. Always pick passwords of at least 16 characters. Consider adding symbols or numbers between or within words only as a means to increase length, since both symbols and letters are of the same level of complexity to a computer. For example, "bluepiecatboatlife" is just as complex as "blue*pie@cat)boat~" because of the character count, not the composition.

Management and Control

Password management and control involves ensuring that users always select unique passwords in compliance with company policies. This usually means assigning a temporary password when creating new user accounts and forcing users to change to a unique password at their first logon attempt. You must enforce password complexity and length restrictions through the operating environment. Otherwise, users will become lazy and not stick with company password regulations unless forced to by the IS environment. Password expiration periods should be enforced as well.

It is also a good idea to regularly audit your users' passwords using both a commercial password auditing tool and a selection of hacker or open source cracking tools. Every discovered password must be changed. However, this process is useless unless you are training users in proper password selection and use. Often, companies will require a short refresher course for all users whose passwords are discovered via a password audit.

Access Control Techniques

Access control techniques are the theories and concepts behind how access is managed within a secured computing environment. Access controls define the relationship between and interactions of subjects and objects (i.e. users and resources). There are two common examples of this: DAC and MAC.

Discretionary Access Control

Discretionary access control (DAC) is the form of control you might be most familiar with, since every commercial OS supports DAC. DAC is based on the discretion or decisions of a user. Often, this user is the environment or resource owner or an administrator, and as such, they get to make a choice about whether or not a user needs access to a specific resource and what type of access is needed. Furthermore, when access is specifically granted (or specifically denied), the user's identity is added to the ACL (Access Control List) on the resource. Thus, access is identity focused and based on user decisions.

Mandatory Access Control

Mandatory access control (MAC) is different than DAC in two ways. First, MAC does not provide for the decisions of users, and instead, access is granted based upon a set of pre-defined rules. These rules are called classifications within an MAC environment. Classifications assigned to resources can be called sensitivity labels. Classifications assigned to users can be called clearance levels. Second, MAC does not focus on user identity, but simply on the classification label on the subject or object. MAC environments are often hierarchical, which means a subject with a high level of clearance can access objects at his level and at all levels below. MAC environments can be compartmentalized, so that each level is separate and distinct from each other (thus no hierarchy). MAC environments can also be hybrids of both, where resources within a security domain or level are compartmentalized, and to gain access, subjects must obtain formal, need-to-know approval based on their work tasks to gain access to the sequestered resource.

Access Control Lists

ACLs (Access Control Lists) are the security mechanisms on objects within DAC environments, where explicit access or denial permissions are defined for users and/or groups. Each entry in an ACL is called an ACE (Access Control Entry). Each ACE focuses on a single user or group but may have one or more access or denial permission settings.

Principle of Least Privilege

The principle of least privilege is the concept of granting users the minimum levels of access required to perform their work tasks, but no more than that minimum. Sometimes the concept of time-dependency can be included as well, so privileges are assigned temporarily and will expire when a project or work task is completed. This concept is primarily focused on privilege, the ability to make changes to resources. Thus, by limiting the objects that a subject can modify, you are effectively protecting the integrity of all other objects. This principle can be applied to all users; however it is often called separation of duties when applied to administrators.

Segregation of Duties and Responsibilities

Segregation of duties and responsibilities, or separation of duties, is the application of the principle of least privilege to administrators. In this concept, each administrator is granted only those privileges that are needed for their specifically assigned administrative tasks. This concept also requires that there are no (or at least very few) full-access, full-privilege administrators. Instead, each administrator is assigned a specific sub-set of admin tasks that they are to perform, for which they are held responsible. Administrators are granted only those permissions, privileges and rights needed to accomplish the specifically assigned work tasks. In this way, fraud and abuse is reduced because administrators don't have sweeping privileges across the environment. In order to compromise the entire infrastructure they will be forced into collusion. Collusion is the act of convincing others to participate in unethical, security violating, possibly illegal activity since the perpetrator is unable (or unwilling) to perform the act alone.

Account Administration

Account administration is the concept of controlling user accounts in order to support the general idea of accountability. This requires strict adherence to an organizational security policy.

Account, Log and Journal Monitoring

All aspects of user activity need to be audited or monitored. This assists in the accountability mechanism by providing the audit logs/trails needed to verify compliance with security policy and detect violations. However, in addition to recording account activity, you must also monitor the logging activity itself. A common attack focus for an intruder is the auditing or logging system since that system records evidence of intrusions and subsequent unauthorized activities. Many intruders seek to disable, purge and scrub the logging system and its associated files in order to hide their actions and prevent detection. A way to counteract these types of auditing and logging attacks is to employ additional monitoring of the logging system, backing up log files regularly or even consider using WORM (write once read many) devices to store log files.

Access Rights and Permissions

Access rights and permissions are the two categories of privileges that are granted to user accounts. A **permission** or a privilege is usually a capability granted to a user over a resource object, such as the ability to read, write, change or print. A **right** is usually a capability granted to a user over the operating environment itself, such as the ability to install software, change system time, reboot the host and update device drivers.

Access Control Models, Methodologies and Implementation

Access control administration can be performed in at least two ways: centralized or decentralized. Centralized access control is the idea that all administration tasks can take place or be performed in a single (or very few) locations. These tasks, however, affect and control the entire environment. This can occur when there are central authentication, authorization and security management servers. Decentralized access control is the idea that all administration tasks take place on each individual system, where the effects and the control are to be local. This requires the admin to physically (or remotely) control each end-system individually.

There are many environments which are a combination of these two concepts. For example, Windows OS based domain environments are both central and decentralized at the same time. This is due to the network being centrally managed by Active Directory domain controllers, while still allowing end users on domain member systems to share resources and control who gains access to their personally shared assets.

Centralized access control is sometimes referred to as remote access control. This makes sense, provided you can picture all of the remote access clients being spread across the globe, while the network they connect to is in a single, "centralized" location. Thus, all of the restrictions imposed by the network are, therefore, centralized. Common examples of centralized access controls that focus on remote access include Remote Authentication Dial In User Service (RADIUS) and the various forms of Terminal Access Controller Access Control Systems (TACACS, XTACACS and TACACS+).

File and Data Owners, Custodians and Users

There are generally recognized six primary security roles. They are:

- **Senior Management** - has ultimate responsibility for the success or failure of a security endeavor and assigns the tasks of security to other roles;
- **Information Security Officer** - designs, implements and maintains the security infrastructure;
- **Owner** - assigns classification labels to objects (e.g. files and data), based on the objects' value to the organization and overall sensitivity;
- **Custodian** - secures objects based on assigned labels within the security infrastructure;
- **User/Operator** - performs work tasks in accordance with procedure and security policy;
- **Auditor** - monitors the environment for security compliance or violation.

Methods of Attack

There are many methods of attack which can be employed by external intruders, internal disgruntled employees and even by penetration testing teams. The following sections review only a handful of the most common attack methods.

Brute Force

Brute force is the attack method which tries every valid possible combination in order to break a security measure. Brute force is often associated with both password cracking, as well as encryption breaking. In terms of password cracking, a brute force password cracking tool generates potential passwords by trying every character, in every position, of a password, throughout its length. Starting with one character, then two, then three, etc., the brute force attack method will always be successful given enough time. Similarly, when an encryption key is to be broken, the brute force attack tool generates a potential key and tries

it against the encrypted object. The attack tool will attempt every possible valid value for the key in the keyspace of the employed cryptography; thus, eventually, it will find the actual key used. Fortunately, brute force attacks against long passwords (i.e. 16+ characters) and long encryption keys (i.e. 128+ bits) are usually time prohibitive for the attacker, as the attack could take many years to complete.

All forms of password cracking, including brute force, dictionary, hybrid, etc. all must convert a potential password into a hash in order to compare it with a stolen password. In all modern and secure environments, passwords are always stored and transmitted in hash form only. Hash is a one-way function and cannot be reversed. When a user performs a valid login, they type in their password, the client hashes that password and then transmits the password to the authentication server. The authentication server then performs a comparison between the current submitted password and the password stored in the user's account in the authentication database. Both the submitted password and the stored password are hashed. Thus hashes are compared, not the original characters of the passwords. The comparison is performed using the Boolean operation of XOR. If the result is 0 (zero), then the passwords are the same and the user is granted logon. If the result is anything else, the passwords are different and the user is denied logon.

Password hashes

Password hashes can be collected or captured in a number of ways. First, a sniffer can capture the authentication traffic of a logon and extract the password hash from the network packets. Second, the accounts database file can be accessed if the attacker can gain read access over the file. Third, the accounts database file can be pulled from a backup.

Denial of Service

Denial of Service (DoS) is a spectrum of security attacks, which is really made up of hundreds of unique attack tools and methods. DoS attacks can be roughly divided into two types: flaw exploitation and traffic generation. Flaw exploitation DoS attacks take advantage of a flaw in some software. This could be the OS itself, installed software, active services or even the network protocol. The goal of a flaw exploitation DoS attack is to crash, lockup or freeze the target. Once the flaw is discovered, it can be patched, thus making the target no longer vulnerable to that *specific* exploit.

Some common examples of flaw exploitation DoS attacks include WinNuke, Ping of Death, Land Attack, and SYN flood.

Traffic generation attacks generate unwanted traffic and direct it toward a victim. The goal of a traffic generation DoS attack is to fill the communication pathway so that legitimate traffic cannot occur. As a victim of a traffic generation DoS attack, there is little that can be done other than wait out the generated traffic, or flood. These types of attacks must be blocked and filtered by upstream providers in order to prevent the malicious result.

Some common examples of traffic generation DoS attacks include Smurf and Fraggle.

Dictionary

A dictionary attack is a form of password attack where lists of possible or potential passwords are used to discover, or crack, the target victim's password. Each password in the dictionary list is hashed, one at a time, and compared to the victim's password. The process is much the same as that of a brute force attack, except that instead of generating passwords on the fly, potential passwords are pulled from a pre-defined list.

There are thousands of dictionary password lists in “the wild” of the Internet. Often an attacker will research and phish against his target(s) in order to learn enough about the victims to select the most appropriate dictionary lists. Dictionary lists often focus on a topic or issue, such as industry, age, education, interests, hobbies, children, vehicles, travel, etc.

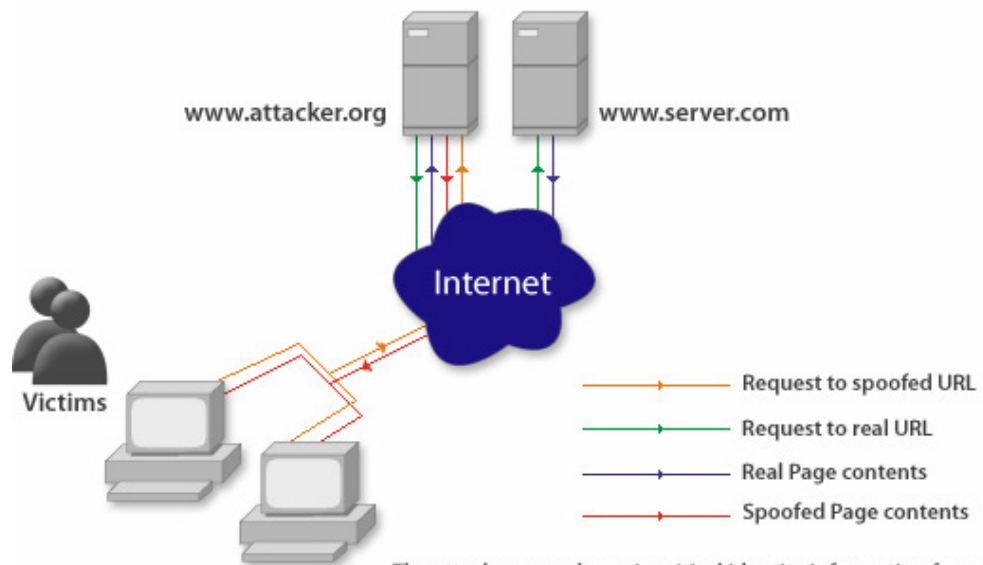
If a straightforward dictionary attack fails, a hybrid attack can be waged. A hybrid attack applies aspects of a brute force attack to the dictionary attack process. It begins with the dictionary lists but changes each potential password by a single character, either adding a character in various positions or replacing a character. If the single character change, called a one-up password, fails, then a two character change is attempted, and so on.

Spoofing

Spoofing is the faking of information. Usually, spoofing means the faking of source identification information. A spoofed packet often has a false source IP address or MAC address. A spoofed e-mail often has a false source e-mail address. The spoofed source can be a non-existent entity, so a reverse DNS lookup would fail and thus identify spoofed messages. However, the spoofed source can be a real entity, so that a reverse DNS lookup is successful. This later spoof is common, since it can mislead investigators by causing them to suspect someone innocent of the malicious activities.

Spoofing is a common element of modern attacks. It offers improved anonymity to the attacker, while increasing the likelihood of attack success. This is brought on through the use of social engineering and phishing activities, which collect information about a target and the target's trusted communication partners/sources. Then, attack packets can be crafted to look like they come from a trusted source.

Man-in-the-middle attacks



The attacker may also gain critical identity information from the victim during the attack. In the case where web page content is unaltered the victim may be totally unaware of the attack.

Man-in-the-middle (MitM) attacks are a form of communications attack. A MitM attack requires the attacker to set up a spoofing attack first in order to mis-direct the communication setup between a legitimate client and server (or sender and receiver). The attacker must steal the identity of the intended receiver/server and/or poison the local DNS or routing system. In any event, the goal is to trick the client/server into sending their initial packets to request a communication session to the MitM attacker, rather than the legitimate server/receiver. Once this is successful, the MitM attacker himself establishes a communication link with the legitimate server/receiver by impersonating the legitimate client/sender. Once this multi-step process is complete, a communication pathway exists between the legitimate client/server and the MitM attacker, as well as between the MitM attacker and the legitimate server/receiver. Even if those communication pathways are encrypted, such as with SSL or a VPN protocol, the MitM is a "valid" participant in those encrypted communications. All traffic between the two legitimate partners passes through the MitM's system in clear form. This allows the MitM attacker to eavesdrop on what is supposed to be an encrypted session and may even allow the manipulation of packets *within* the session, to keep the ruse sustained.

Spamming

Spam is unwanted, unrequested, often inappropriate messages sent to your e-mail inbox or posted to a discussion forum or public blog. Spam can be a single message, or a flood of messages. Spam is used for several purposes by attackers. First, it can be a form of mass advertising. Second, it can be a way of performing a DoS against a message system. Third, it can be the first step in exploiting a target user through social engineering and phishing in order to steal an identity or gain unauthorized access to a secured environment.

Spam filtering is currently the most effective method of preventing spam. Unfortunately, spam filtering will often filter or block legitimate messages. Therefore, regular inspection of the filtered traffic must be performed in order to rescue legitimate messages before they are purged from the environment.

Sniffers

A sniffer is a form of network packet capturing tool. Sniffers have legitimate uses, such as diagnosing network health and resilience testing. However, in the wrong hands, a sniffer can be used to collect network communications without authorization. Some of the primary targets of sniffing are user logon credentials. As previously discussed, once a user's password hash is captured via sniffing, it can be cracked offline. Sniffers can also extract the contents of packets in order to reproduce the original data or communications.

This kind of sniffing is referred to as eavesdropping.

Countermeasures against sniffers include deployment of a switched based network, using only encrypted protocols and applications, and regularly checking for devices in promiscuous mode.

Crackers

A cracker is a term used to describe a malicious hacker. The term cracker is often meant to indicate that the person performing the technical activities is a criminal. The term hacker is often meant to indicate that the person performing the technical activities is not a criminal, but just an intelligent and curious computer geek. In the media and in off-the-cuff conversations, the terms hacker and cracker seem to be used to both mean an unwanted and possibly criminal user.

The term cracker can also be used to loosely describe those attack tools which crack, extract, discover or guess passwords, encryption keys or other elements used to bypass access controls. For example, brute force and dictionary attacks are forms of crackers.

Monitoring

Monitoring is the process of overseeing the activities that occur within an environment. Monitoring, logging and auditing are all terms used to define the process of collecting records of activities and events in order to check compliance with security policy and discover any violations.

This topic is covered more in depth in the **Audit and Monitoring** domain later in this exam manual.

Intrusion Detection

Intrusion detection is the act of watching network and system activity, and investigating audit logs for patterns or symptoms of unauthorized activity. The goal of an Intrusion Detection System (IDS) is to find, stop and identify intruders or any other form of unwanted access or activity.

Alarms and Signals

An alarm is a notification to administrators or other authorities that an intrusion is taking place (or in some instances has already taken place). An alarm can be tied to a physical intrusion system, which indicates that a trespass is occurring. Or, an alarm can be tied to the IT environment which indicates that an unauthorized logical connection has been established (or attempted). Some alarms are silent so as not to notify the intruder that their presence has been detected. A silent alarm gives authorities time to respond, in the hope of capturing the intruder.

A signal is another informative action that an IDS can utilize to keep track of occurrences. For example, when an IDS detects an intruder, it can record the event to a log file, notify the administrators via e-mail, screen pop-up and/or pager code. Often once an intruder is detected, the IDS will turn on additional auditing and logging systems to record as much information as possible about the intruder in order to learn who they are, what they are doing, how they obtained access, and what exploits are being used.

Audit Trails

Audit trails are the result of auditing. Often, auditing is an ongoing activity that all users, authorized and unauthorized alike, know about. In fact, a warning banner about monitoring and unauthorized access is usually presented to users at each logon entry point. Thus, everyone is made aware that their actions are being logged, that and any violation of security policy will be punished. Auditing, therefore, is a form of preventative control. However, the audit trails that are created by auditing are a form of detective control, as an administrator can review them to detect, discover and reconstruct the events related to a security breach.

Audit trails are essential security tools. Without audit trails there would be no evidence of either authorized or unauthorized activity. Within IT, audit trails are your primary source of evidence in relation to incidents, breaches and outright computer crime. Audit trails should be protected and backed up regularly. In fact, a live audit trail file is the most vulnerable to intruder manipulation and attack.

A common activity of intruders is to disable the auditing system and purge the audit logs of all entries related to their intrusion. There are very few ways to ensure that audit log purging does not occur. One method, as discussed previously in this manual, is to write the audit logs directly to a storage media that is a WORM (write once read many) device. The WORM device ensures that once a log entry is written, it can never be erased or changed. A second method is to have another system maintain a real-time copy of the audit logs.

Once audit logs are closed, they should be hashed, digital signed and stored on write-protected media in a very secure location. Keeping audit logs is the only way to ensure that evidence about an event in the past is still available for an investigation.

Violation Reports

A violation report is one of two possible concepts. First, a violation report can be the output of a clipping level auditing system. In a clipping level auditing system, errors are monitored in various systems, applications, services, hardware, etc. Whenever the number of errors exceeds a pre-defined limit or threshold, a violation record is produced. This threshold is called the clipping level, and it is the level at which the number of errors goes from routine, normal and expected to unique, abnormal and suspicious. The process of evaluating violation records produces a violation report.

Second, a violation report can be an incident report. An incident report is the output of an IDS or audit log data mining operation which shows the details of a security violation, system breach or intrusion.

In both cases, the violation report is a detailed, concentrated collection of information about unwanted events that occurred within a secured environment. This information should be properly controlled and revealed only to those parties with a need-to-know, such as senior management and the information security officer involved in the investigation or response (i.e. containment and repair).

Penetration Testing

Penetration testing is the concept of testing the security of an environment to determine how well it repels attempts to penetrate its protected boundaries. Penetration testing is also known as security assessment or ethical hacking. Ultimately, penetration testing is the use of hacker skills, techniques and tools to attempt intrusions and other forms of security violations in order to evaluate the strength of deployed security solutions. Penetration testing should only be performed with specific written approval from senior management. Also, penetration testing should only be performed by experienced professionals who thoroughly understand their tools and techniques and the possible consequences of finding vulnerabilities in their targets. Since penetration testing is basically approved hacking, there is a significant possibility that the testing process will damage the target systems or generally affect uptime, productivity, etc.

Penetration testing can be performed by attacks teams with various levels of knowledge about the target:

- A full knowledge team knows everything about the target, usually because they are the company's information security team or IT staff. They are the least costly, and can perform their testing in the least amount of time, but they usually don't offer real-world hacker perspectives on the organization's state of security. A full knowledge team may have blind spots and may face conflicts of interest.
- A partial knowledge team is an external team who has been given documentation about the network infrastructure and production environment. They are more costly than a full knowledge team and will take longer to perform their tests. However, they offer a more realistic real-world hacker perspective on the organization's state of security.
- A zero knowledge team is also an external team, but they have no knowledge of the target environment. They must learn everything from scratch, like a real-world hacker. As a result, they provide the most realistic real-world hacker perspective on the organization's state of security. However, they are the most expensive and will take the most time to perform their tests.

Penetration testing usually involves five primary phases or steps:

- **Discovery** – a phase using passive actions only to perform discovery, footprinting and reconnaissance of the intended target. Any and all public information sources are used, but no methods that are obviously attacks are employed. All interactions with the target are benign.
- **Scanning** – active actions are used from this phase forward. The goal of this phase is to construct a map of the target's network, including addressing scheme, function or roles of devices, as well as OS, services and deployed applications.
- **Vulnerability mapping** – based on the scanning results, all potential vulnerabilities in the target systems are tested to create a mapping of all open, unpatched and unprotected weaknesses in the target.
- **Exploitation** – exploitation of one or more target weaknesses are used in order to gain entry into the target network, often this means impersonating a user through a weak user account. Once access is obtained, the intruders perform privilege escalation; plant attack tools, rootkits, back doors or other forms of malicious code; create or manipulate user accounts; inventory the storage media; purge the auditing system; then exit the now compromised system.
- **Documentation** – the attack team documents every step, every action, every tool, every keystroke, every success and failure, every single small detail of information encountered, discovered, collected or stolen and presents this final report to senior management. This final report also contains recommendations on how to improve security to prevent similar real-world exploitations from occurring.

Administration

Security administration is both the collection of daily activities, as well as long term concepts that are implemented in a total solution which are designed to manage and maintain security.

Security Administration Principles

Security administration principles are the foundational concepts and ideas of security. Reliable, real-world security solutions are built on these foundational concepts.

Privacy

Privacy is a form of confidentiality. Privacy is a level of secrecy, isolation and seclusion protection individuals assume or are provided in regard to information, data and activities deemed personal. The idea is that activities and information related to the person should be kept confidential from other persons, as well as from an employer. In most commercial organizations, users often assume privacy when there is none. In government/military environments, a significant amount of privacy is provided for by government regulations. It is the responsibility of end users to fully understand the level or lack of privacy protection afforded them, before using an employer owned IT system for personal activities.

Confidentiality

Confidentiality is the protection against disclosure. Disclosure is the revealing of information to unauthorized entities. Confidentiality is therefore the prevention of *unauthorized* read or proximity access alongside the support of *authorized* read or proximity access.

Integrity

Integrity is primarily the prevention of unauthorized and unintended change. Integrity is also the support of authorized and intended change. Integrity can also be viewed as the assurance that stored information is a true reflection of reality and represents the highest source of truth. Integrity violations are known as corruption, alteration or destruction.

Availability

Availability is the protection of the ability for workers to perform their work tasks and gain access to valid resources. Availability is therefore the protection of bandwidth and timeliness, so that systems and networks provide adequate capacity for necessary and predictable performance levels. Violations of availability are known as destruction and/or obstruction.

Authorization

Authorization is the collection of access controls, permissions, privileges, user rights and capabilities assigned to users, all of which define what the user can and cannot do within a secured environment. Authorization defines exactly what users are authorized (or not authorized) to do. Authorization is implemented within the confines of the imposed access control concept (i.e. DAC, MAC, RBAC, etc.) and should be governed by the principles of least privilege and separation of duties.

Identification and Authentication

Identification is the claiming of an identity. Authentication is the process of proving that you are the authorized user of the claimed identity. Identification and authentication are the first two steps towards accountability. A single factor is used for the purpose of identification. One or more factors can be used for the purpose of authentication. Using two or more different factors always provides more security than limiting authentication to a single factor.

Accountability

Accountability is the concept holding a person responsible for the actions of the digital user account to which they are assigned. Accountability only makes sense, and only becomes legally enforceable, when the authentication process of the environment is a truly secure, two-factor or multi-factor system. The five steps of accountability are: 1) Identification, 2) Authentication, 3) Authorization, 4) Auditing, and 5) Accountability. The fifth step, accountability, is the use of a security incident, assessment or reporting tool to perform data mining operations on audit logs in order to detect violations of security policy.

Non-repudiation

Non-repudiation is the protection against users being able to deny sending a message or performing an action. If accountability is properly imposed, no user can repudiate any action recorded by the auditing system which is attributed to them. Non-repudiation relies upon strong authentication, as well as protections against impersonation.

Data Classification

Data classification is the labeling of resources and assets with a classification label. A classification label is a letter, number, word or phrase used to describe a specific level of security within a specific environment. There are two commonly recognized classification schemes: government/military and private sector/corporate business. A classification scheme divides up the environment into a finite number of security domains, layers or levels, each with a unique label. A data classification label is often called a sensitivity level. The classification label indicates the value of the data to the organization and defines the level of security protection that a custodian must provide the resource. When the same label names are applied to subjects, the labels are called clearance levels.

Documentation

Documentation is the collection of all written and recorded information in regard to an organization's security. This includes all security policy documents, incident reports, audit logs, etc. Exhaustive and extensive security documentation is a key aspect of a long term, successful security endeavor. Ultimately, the goal of a security solution is to fully document every action and event so that there are no unexpected occurrences or fully reproducible actions, which, in turn, prevents any unintended consequences.

Audit

To audit is to record events that occur within the OS and installed software, usually in relation to user accounts interacting with the environment. The purpose of auditing is two-fold. First, auditing serves as a preventative control, as watched users are less likely to knowingly commit a security violation. Second, auditing produces audit logs which can be used to detect security violations. Auditing can also be called logging and monitoring.

CIA Triad



The CIA triad is a shorthand term used to refer to the three primary security services of confidentiality, integrity and availability. The order of the letters, with "C" being the first, indicates that the environment is more concerned about confidentiality than any other security service. Likewise, when the AIC triad phrase is used, this indicates a preference towards availability protections. In general, all three security services should be properly addressed in order to establish a reasonable and worthwhile security solution.

Security Architecture

Security architecture is the implementation of software development controls that ensure a more reliable product by ensuring that security concerns are imbedded throughout the development process. Generally, when security is initiated at the beginning of a new concept and is managed and addressed in conjunction with the development process, security is more likely to be reliable and cost effective.

Design objectives

The primary design objective is to ensure that a finished product not only performs the necessary functions for which it was created, but that it performs those functions securely. A finished product should provide confidentiality and integrity protection for the data it interacts with, processes and stores. That product should also interoperate and cooperate with availability protections to ensure that work tasks can be accomplished in a timely manner.

Development life cycle

The development life cycle is the six phase process that all products go through from conception through the end of their productive life. The six phases, or stages, of the development life cycle are:

- **Project Initiation** – the conception and definition of the project, which includes an initial proposal, concept study and risk assessment;
- **Functional design analysis and planning** – the requirements of function and security are defined, system environmental specifications are defined;
- **System design specifications** – the requirements of data, function and behavior are defined, design elements for information storage structures, architecture and procedure are specified;
- **Software development** – code is developed, testing is designed, debugging is performed, formal testing is completed and a finished product is produced;
- **Installation** – product is distributed and installed into production;
- **Maintenance** – ongoing use, administration and maintenance of the product, including reconfiguration, patching, upgrading, auditing, certification and accreditation.

At the end of the six phase development life cycle, the three remaining options are revise, replace or retire.

Security control architecture

Security control architecture is the collection of security controls embedded into the environment, the supporting platform and even the system design of an IS. The following items are part of this architecture:

- **Process isolation** – the restriction placed on processes so that they are unable to access hardware directly, are unable to interfere with the memory spaces used by other processes and are forced to communicate with the reference monitor in order to interact with system resources.
- **Hardware segmentation** – the act of segmenting hardware in order to provide for process isolation, often by dedicating memory modules and CPUs to specific processes.
- **Separation of privilege** – the restriction of processing privileges to limit the damage that a rogue or corrupt software module might cause.

- **Accountability** – tracking the activity and events of all elements of a software environment in order to link results to their causes.
- **System high** – a mode of system operation where compartments of resources are inaccessible to some processes which have not been assigned the need-to-know.
- **Security kernel** – the protection mechanism coded into an operating system that performs the functions of the reference monitor concept.
- **Reference monitor** – the reference monitor serves as the access control mechanism which restricts communications across the security perimeter. The security perimeter is what is separating the components of the Trusted Computing Base (TCB) from the remainder of the computing system.

Protection mechanisms

Numerous mechanisms exist which can be used to assist in the protection of system integrity, database integrity, operating system integrity and system confidentiality. These include:

Layering and Data Hiding

Layering is the lattice ordering of related security domains, such that they represent a hierarchy of access from low to high. The use of layering allows for the assignment of classification labels to objects and subjects. By placing an object in a layer that is higher than the clearance of a subject, that object is effectively hidden from the subject.

Abstraction

Abstraction is the concept of obtaining a more general, less detailed perspective. A common example of abstraction is to work with groups of users rather than the individual users. Another example is to test a newly written program using black box testing measures, which does not see the internal logic of a system. This is opposed to the use of white box testing measures, which examine the detailed internal logic of a solution. Another example is to view a completed program as a single functioning entity, rather than viewing the individual objects, or the lines of code that constitute those objects.

Modes of operation

An operating mode is the state of access a user is assigned based on their privileges and permissions. A “supervisor mode” state is capable of more expansive activities, such as modifying the environment through re-configuration or software install/removal, than a “user mode,” which is limited in the scope of its capabilities. User mode allows a user to perform necessary work tasks while protecting the stability and security of the overall operating environment.

Data/information storage

Primary storage (or real storage) is what is commonly called physical RAM. Primary storage holds information that is associated with currently active applications. Most primary storage mechanisms are volatile. Volatile storage loses its contents when power is lost.

Secondary storage is what is commonly called persistent storage, such as hard drives, floppy disk drives and burnable CDs and DVDs. Secondary storage is 100 to 1000 times slower than primary storage, but it is usually non-volatile.

Virtual storage, or virtual memory, is the combination of primary storage with secondary storage to artificially create a larger amount of addressable memory space for active applications. Virtual storage implementations involve the process of paging. Paging is the process of switching out sections of memory between primary storage and secondary storage as those sections of memory are required by the CPU or active applications. Each time paging occurs, the performance of the system is affected, often significantly.

Random storage is a type of storage where information from the storage mechanism can be read randomly, rather than forcing a sequential read. Random storage often is indexed by a master file table, which is used to discover the exact location of relevant data in order to direct the read/write function directly to that storage location. Most storage devices are random storage.

Sequential storage is a type of storage that requires front to end reading of the storage media in order to locate, retrieve and write data. Tape storage is sequential storage.

Configuration Management

Configuration management is the management or control of change. Change is bad if that change causes unintentional diminishment of established security. Therefore, to prevent bad change, all change must be managed and controlled. Changes should be thoroughly tested and evaluated before being implemented into production. Configuration management attempts to prevent unintentional diminishment of security by allowing only tested and approved changes into the production environment. The change control process also attempts to provide a rollback path in the event of an unintended consequence of an applied change.

Data Classification

Data classification is the act of assigning labels to objects (and/or subjects) to indicate the level of value, sensitivity and required security protections. The objectives of a classification scheme are to prevent disclosure and to control access. Data is assigned a classification after being evaluated or compared to classification criteria. Classification criteria are a set of characteristics which are of concern. If an object elicits a certain percentage of the classification criteria, it will be assigned one of the classification labels related to that object's strata of security needs.

A commercial data classification scheme is often defined as a four-layer or level scheme: public, sensitive, private and confidential (proprietary).

A government/military classification scheme is often defined as a five-layer or level scheme: unclassified, sensitive but unclassified, confidential, secret and top secret.

Data classification criteria often include a valuation of that data. The value of data is dependant upon both tangible and intangible elements. The tangible elements of worth include purchase price, licensing fees, maintenance fees, upkeep costs, protection costs, training costs, repair costs and administrative costs. The intangible elements of worth include profitability, improved productivity, market share, public opinion, speed of recovery, advances in research and development, protection from competitors, competitive edge, exclusivity, free market value and intellectual property.

Information/Data Collection and analysis techniques

Information or data about people, resources, networks or organizations can be collected through a wide number of techniques. These include: intrusion detection systems, penetration testing, scanning, probing, demon dialing (war dialing), war driving, violation analysis, vulnerability analysis, sniffing, dumpster diving, social engineering, auditing, violation analysis and more.

Employment Policies and Practices

People are the weakest link in security. An environment is only secure as the most intelligent and capable administrator and the most ignorant and uncaring end user. An authorized insider can almost always find a way to thwart logical, technical and physical security protection mechanisms. Therefore, we must build security solutions designed specifically to protect the organization from insecure personnel, as well as intentional and unintentional malicious events.

Distinct job descriptions should be written for each and every personnel position. This defines what is needed and required for each position. When new hires are needed, the job descriptions should be used to drive the new recruit selection process. Only those applicants that meet the minimum requirements should be seriously considered for a specific position. Once initial selections are made, background and security checks should be performed relative to the job position and the security level of the data that such an employee will come in contact with. When a qualified applicant is found who meets all pre-screening requirements, they should be presented with employee documentation and agreements. These should include the standard security policy, acceptable use policy, monitoring/auditing agreement, non-disclosure agreement, and any other relevant documentation that the new employee needs to read, agree to and sign.

During the course of the employee's employment, they will be subject to supervisory oversight and regular reviews. In the event of misconduct, poor reviews or security policy violations, the employee may be subject to job action warnings. If the warnings are not sufficient to change the employee's behavior, termination may be necessary. When an employee is to be terminated, a form of exit interview should be conducted.

An exit interview is a firing process where the employee and the employer are protected and dignity is maintained. The employee is invited into a private meeting room with their manager and a witness (often a security guard or another manager) where they are informed of the termination of their employment. The ex-employee is asked to return their keys, smart cards, access devices, and company owned equipment. The ex-employee's user account and all facility access codes are disabled or revoked. The ex-employee is asked to re-read the NDA and re-sign it. The ex-employee is then escorted off of the premises immediately. Any personal belonging are collected by a security guard and returned off-site.

Other aspects of personnel management include the application of the principle of least privilege, separation of duties and job rotation.

Policies, Standards, Guidelines and Procedures

A complete security policy is comprised of four types of documents: policies, standards, guidelines and procedures. A **policy** is a long term visionary document describing the general state or goals of organizational security. A **standard** is a collection of requirements that define how hardware and software are to be used in an organization. These requirements may be regulatory, technology, industry, best practice or self-imposed. **Guidelines** are general concepts on how to accomplish various tasks which are used specifically to create procedures. **Procedures** are detailed, step-by-step instructions on how to perform specific tasks.

Roles and Responsibilities

There are several important roles within a secured infrastructure. Each role has a set of specifically defined responsibilities. These roles and responsibilities are defined within the security policy documentation and are ultimately assigned to organizational personnel.

Senior management has the sole responsibility for the success and failure of the security endeavor of an organization. All business operational decisions, i.e. deciding on the structure, direction and content of the security policy, are to be made by senior management.

The IS/IT security department designs and builds the secure IT infrastructure of the organization. They must perform their tasks under the watchful eye and approval of senior management.

An owner brings resources to the secured environment. It is the task of the owner to define and justify the value and security requirements of each resource object through the security policy prescribed by classification criteria.

The custodian receives the value labeled object from the owner and places it in the correct security container that was built by the IS/IT staff. Thus, the custodian ensures that the necessary protections of an object are provided through proper use of the IT infrastructure.

Once resources are secured, users or operators can interact with the environment to perform their work tasks in accordance with organizational security policy.

While users are performing work tasks, auditors can oversee the environment to check compliance with security policy and to detect the occurrence of violations.

Security Awareness Training

Simply having a security policy is not sufficient. All employees must be familiar with the foundational and universal elements of that policy, as well as their job task specific compliance requirements.

The first stage of security education is awareness. Awareness is the education of common sense, and of the foundational and standardized security elements that all members of an organization must adhere to.

The second stage of security education is training. Training is job task or job role specific security training. Usually both awareness and training are provided by the organization.

The third stage of security education is education. Education is the obtaining of broad understanding about a wide variety of security topics. Often education is not specific to a current work task. Education is usually sought outside of the organization and may be associated with certification.

Security Management Planning

Security management planning is simply the concept of planning out every aspect of an organization's security infrastructure and business processes. This is often visible through the written security policy documentation. Performing the planning of security is evidence of due diligence. Implementing a developed security policy is evidence of due care.

Data/Information System Attacks

There are innumerable variations of attacks directed at IS and its hosted data. A significant portion of any security policy are those countermeasures and safeguards selected or designed specifically to thwart one or more of these attacks. The following sub-sections describe several of the more common forms of IS and data attacks.

Hidden code

Hidden code is simply the idea of planting unseen and unknown malicious code into an IS so that security violating events take place. Hidden code can take the form of a virus, logic bomb, Trojan horse, asynchronous attack, etc.

Interrupts

An interrupt can often be recognized as a system freeze or lockup. The purpose of an interrupt attack is to cause either a single application or the entire system to stop processing.

Remote maintenance

Remote maintenance, remote access, or even remote control are all problematic when an unauthorized user can gain configuration or management control over a process or system through a logical connection. Remote maintenance is sometimes made possible by the vendor, who purposefully, or by oversight, includes such features. For example, when a debugging tool is accidentally left imbedded in source code. Remote maintenance attacks can also be made possible through the planting of hacker tools and back door code.

Logic bomb

A logic bomb is a form of hidden or planted code that waits dormant within an IS waiting for a triggering event, such as a specific time and date, the execution of a program file, or a behavior or action of a user.

Trap door

A trap door is similar to a Trojan horse, however instead of the malicious code gaining immediate access to the target system upon execution of its host container program, a trap door remains dormant until the user stumbles across the trigger or trap that releases the malicious event.

Browsing

Browsing is the act of accessing or viewing data that is outside of an official area of responsibility, granted access level or assigned clearance. Browsing can be rummaging through another users home directories, performing dumpster diving or engaging in shoulder surfing.

Spoofing

Spoofing is the act of faking information. In most cases, spoofing is used to hide the source of information, communications, messages or activities. Some of the more common forms of spoofing involve IP addresses, MAC addresses, and e-mail addresses. When an identity is spoofed, the spoofed identity can be completely false, or it can be used to misdirect blame or suspicion onto an innocent third part.

Exhaustive

An exhaustive attack is usually called a brute force attack. In this form of attack, every possible valid combination or value is tried. Such an attack is always successful, if given enough time to perform all possible permutations. Exhaustive or brute force attacks are commonly used in the act of password cracking or in guessing symmetric encryption keys.

Inference

Inferencing attacks are basically educated guessing attacks. When an inference attack takes place, a data point is used to infer, deduce or guess at another data point. Often the inferred data is more valuable, higher classified or segregated from the attacker's current access privileges.

Traffic analysis

Traffic analysis, also known as trend analysis or covert channel analysis, is the act of investigating the patterns, traffic and trends produced by a system (both IT as well as organizational). Traffic analysis does not examine the contents of communications or element transactions, instead it learns about patterns, trends and time tables. Through traffic analysis, an attacker or auditor can learn about which systems produce or receive the most data, when the most data is sent or received, and when and where encryption is employed.

TOC/TOU

A time of check/time of use (TOC/TOU) attack is a form of replay attack. An attacker uses a sniffer to capture logon traffic (i.e. time of check), then after some manipulation, replays or retransmits the captured packets in hope of creating an authentication communication session with the service target by impersonating the original client (i.e. time of use).

Audit and Monitoring

Auditing and monitoring are the tasks of collecting information about an IT environment and/or a physical environment. The goal of auditing and monitoring is to verify compliance with security policy and detect violations of that policy.

Control types

There are several security control function types that can be used in the protection of valuable assets. These include directive, preventative, detective, corrective and recovery controls. A directive control provides guidance on how to comply with other controls or restrictions. Examples include: Exit signs indicating escape routes, security procedure documentation or security guards offering verbal instructions. Preventative controls are used to prevent or discourage violations of security. Detective controls detect violations of security. Corrective controls attempt to stop security violations and return the environment back to a pre-incident state. A recovery control provides more extensive response to violations and is able to repair damage and restore systems, in addition to corrective control capabilities, in order to restore an environment back to a normal and secure state.

Security Auditing

A security audit is both a procedure and a mechanism to ensure compliance with security policy. An internal audit is the form of auditing that takes place on a consistent basis to oversee the operations of the environment and the actions of users. One standard goal of internal auditing is problem identification. Once a problem is identified, the next step is problem resolution. Problem resolution attempts to minimize the risk of the problem, prevent problem (re)occurrence and prevent system downtime.

External audits are outside consultants brought in to perform an unbiased appraisal of an organization's compliance with their own security policy and with industry best practices. By showing that an organization is in compliance with its own security policy that is itself inline with industry best practices for security, an organization is able to show due care.

The results of internal audits, i.e. audit logs and audit trails, should be reviewed and inspected on a regular basis. Most security experts claim that a weekly internal appraisal of security through audit log analysis is essential. External audits should be performed on a yearly basis in order to sustain and maintain a security policy in step with external changes to the state of security.

In order for any security infrastructure to be successful, it must establish a reliable process by which it holds users accountable for their actions. Accountability is established through strong authentication that resists spoofing and impersonation, tied with a reliable system of access control, auditing and analysis.

Through the detailed inspection and review of audit logs, security administrators can re-construct the occurrences that lead up to an intrusion or other form of security incident or breach. Only through extensive and detailed auditing is reconstruction possible. Furthermore, only audit logs and trails that have proven and established integrity can provide legal proof or evidence of real events.

It is important to clearly define the organizational audit policy and its related retention policy. The audit policy defines what is audited and how it is audited, while the retention policy defines the length of time audit logs will be retained and how they will be stored and protected. It is also important to consider the physical constraints of the storage media, as that may dictate special storage needs, such as avoiding magnetism, controlling temperature, maintaining moderate humidity, etc.

Audit log backups should be stored to protect against alteration, damage and theft. Live audit storage media should have availability protection to ensure that all audit events can be stored properly. Likewise, stored audit media (i.e. audit log backups) should be protected in order to ensure their availability when a historical investigation of previous events is performed.

Audit log backups should be stored offsite daily, weekly at most. Offsite storage should provide access control and protections against damage. This should include fire protection.

Monitoring tools and techniques

There are many ways to monitor and oversee the security of an organization.

Warning banners

Warning banners proclaim to all visitors that unauthorized access is prohibited and all access is monitored and recorded. Furthermore, warning banners usually state that any unethical, illegal or security compromising behaviors will be reported and prosecution pursued. Thus, warning banners are not themselves a form of monitoring, rather they are an announcement to users that monitoring is occurring.

Keystroke monitoring

Recording keystrokes can be a form of monitoring used to detect abuse or impersonations.

Traffic/trend analysis

Traffic analysis or trend analysis is the act of watching for patterns in the communications of an organization. Such patterns might not reveal the contents of the communication, but can reveal the identity of the communication partners, the amount of data and the time and length of communications. Traffic patterns and trends can be used to detect the use of covert channels.

Event monitoring

Event monitoring is essentially the same thing as auditing. Often event auditing is a native feature of an operating system. All events, whether they are related to the OS, to services, applications, devices or users, are recorded into an audit log for later inspection and analysis.

Real-time

Real time monitoring occurs by watching for events, activities and patterns in live network communications and active processes. When a real-time analysis detects an intrusion, breach or anomaly, it can trigger an alarm and response to the security incident.

Closed Circuit Television (CCTV)

CCTV, in conjunction with security cameras, is a common form of physical environmental logging. When security cameras are present, they serve as a preventative control. When recorded video is reviewed, it serves as a detection control. CCTV expands the visual range of security guards and provides a tangible record of events.

Intrusion detection

Intrusion detection is the security mechanism that monitors for violations of security policy. Intrusion prevention is a mechanism which attempts to thwart or prevent intrusions from being successful. Often, this is accomplished with strong authentication procedures and network traffic filters.

If intrusion prevention fails, intrusion detection is present to apprehend the intruder. Intrusion detection can focus on the real-time activity of network traffic, or the recorded events of audit logs on a host system. Intrusion detection can recognize security breaches through pattern or signature matching, anomaly detection, heuristic analysis or protocol anomaly detection. When an intrusion is detected, passive and active responses may be triggered. Common passive responses include additional auditing, reverse lookups and administrator notification. Active responses can include session termination, port closing, link disconnect, service termination or padded cell transfer.

Illegal software monitoring

Preventing the installation of unapproved software is a key component of a secure environment. Allowing users to install software will encourage the use of unapproved software, freeware/shareware and illegal or pirated software. Only tested and approved software should be allowed within the secured network.

War dialing

War dialing is the use of a modem dialing tool to discover the phone numbers associated with dial-up modems, answering systems, PBXes and other electronic devices or communication systems connected to a telephone line. Some war dialers will perform dictionary and brute force logon attacks against any discovered computer systems.

Sniffing

Sniffing is the act of collecting network packets. Most sniffers can read the headers of captured packets and produce status and statistics about the network. Some sniffers can extract the payload of packets and re-create the original data. Others can edit captured packets and re-transmit them. Sniffers usually place the NIC into promiscuous mode in order to capture all traffic on a segment, rather than just those packets addressed to the NIC's MAC address.

Eavesdropping

Eavesdropping is the act of listening in on communications. This can focus on voice conversations or network traffic. The latter usually involves the use of a sniffer.

Radiation monitoring

Radiation monitoring, a.k.a. emanation monitoring, is the process of reading the electromagnetic signals produced by electrical devices in order to re-produce the associated data that created the original signals. Emanation or radiation eavesdropping can be performed on copper network cables and many other computer components.

Dumpster diving

Dumpster diving is the activity of sifting through garbage, trash, refuse or other discarded materials in order to collect information about a target organization or individual. The success of dumpster diving can be greatly diminished by shredding and incinerating all paper waste, and thoroughly inspecting and sanitizing computer components before they are discarded, donated or sold.

Social engineering

Social engineering is the act of gaining access or privilege simply by asking for it. Social engineering is a form of attack that focuses on the weakest link in organizational security, namely people. Social engineering can take place in person, via face-to-face encounters, or over the phone. It can also take place through IT, via e-mails, Web sites, chat systems, Trojan horses and a number of other forms of software and communication solutions. The best protections against social engineering are user awareness and information classification.

Inappropriate activities

Inappropriate activities are actions of users/employees which are not necessarily security breaches or even criminal actions, but which may threaten the reliability, or CIA, of a secured environment. Often these actions are defined in an acceptable use policy in order to encourage users to avoid them. Inappropriate activities include wasting resources, hosting inappropriate content, racial or sexual harassment and abusing or not-respecting assigned access and privileges.

Fraud

Fraud is the criminal act of falsifying information. Fraud is a violation of the integrity of business processes and information. Fraud is often an attractive crime because a computer system can make the perpetration of fraud seem easy and undetectable. However, most secure environments are specifically designed to detect fraud and hold users accountable for their online activities.

Collusion

Collusion is the act of conspiring with one or more people to commit a crime or participate in security policy violations. Security preventative measures are often specifically selected to discourage collusion, such as the principle of least privilege, separation of duties and detailed auditing.

Cryptography

Cryptography is the practice of safely securing, storing and transmitting sensitive information, and it outlines the protocols, practices and procedures necessary to build cryptographic components. Ostensibly, the purpose of encryption through cryptographic implementations is to conceal confidential information from exposure to unauthorized parties; in practice cryptography occurs at varying layers of the OSI protocol reference model for various reasons.

Cryptography (also called cryptology) is both a discipline of mathematics and computer science. Crypt-analysis (or "codebreaking") is the discipline of reversing, uncovering or defeating cryptosystems and cryptographic components.

Key concepts associated with strong cryptosystems include:

- Confidentiality – restricted access to authorized parties only
- Authenticity – validation of the origin and identity of a message
- Integrity – assurance that no tampering occurred in transit
- Non-repudiation – a sender cannot deny having sent a message

The appropriate use of cryptography to achieve the desired business effects

Cryptography in a business context is instrumental to maintaining the privacy of business partnerships and secrecy in business dealings. Confidential information exchanges between business-to-business transactions on a regular basis including customer data, proprietary information and the communications of top-level executives, engineers, administrators and so forth.

Securing these entities and operations against eavesdropping, interception and manipulation is best achieved through cryptographic protocols and frameworks. Some of the assurances a good cryptosystem makes are confidentiality, integrity, authenticity or authentication and non-repudiation.

Confidentiality is the assurance that no unauthorized party may observe cryptographic messages and transactions. This is the first principle of the CIA triad first discussed in the administration domain. This also applies to the cryptographic domain.

The second column of the CIA triad, integrity, is the ability for an object to maintain veracity and resist manipulation by unapproved parties. Integrity in computer security is the assurance that an object, message or transaction remains unaltered from its original form during storage or transit.

Authenticity is the assurance that a claimed identity for a message, transaction or object is the original source and said source is permitted to view, modify and deliver that item. Authentication is a means of verifying original authorship or ownership over a given cryptographically secured item.

Once an individual signs, seals and delivers a cryptographic message, his or her identity becomes an integral part of the message. Going forward, ownership cannot be revoked or denied once the message is created and delivered to the intended party. Non-repudiation also applies to cryptographic events created for encrypted networking scenarios and is made possible through a combination of authentication, authorization, accountability and auditing.

Cryptographic concepts, methodologies, and practices

Cryptography utilizes many concepts, methodologies and practices within the context of a secure framework. Depending on the circumstances, level of risk and value of protected information, cryptosystems may be implemented at the physical layer, in the form of highly specialized communications equipment, and up to the application layer, where presumably sensitive content is accessed, created and modified. Basic cryptography terminology includes:

- Encipher – the act of transforming readable text into an unintelligible format
- Decipher – the reverse process of encipher
- Keyspace – the breadth and depth of values used to construct keys
- Plaintext – a message in its natural form, before encryption is applied
- Ciphertext – the result of cryptographic processing of a plaintext message
- One-way function – produces cryptographic values from which the original data cannot be derived
- Cipher – a component that assures confidentiality by rearranging the information in a message to disguise its true meaning or content
- Cryptanalysis – a scientific approach to deriving plaintext material from ciphertext, without knowledge of the key or exploiting weaknesses in the algorithm
- Cryptosystem – cryptographic implementations in hardware and software solutions that convert messages between plaintext and ciphertext

Other cryptography concepts are introduced during the course of this chapter.

Symmetric vs. Asymmetric

There are certain conceptual and technical differences to using both methods of symmetric and asymmetric key cryptography. These subtle differences have significant impacts on security, depending on the nature of the information under protection and the exchange of this information between participants.

Symmetric Key Cryptography

A symmetric key algorithm relies on a distributed encryption key shared among participants in a cryptographic exchange. The same key used to encrypt messages also decrypts messages, giving symmetric key cryptography its name. Although the same key may be used for processing data in both directions (encryption/decryption), there may be a simple transform between instances of said key, depending on the operation.

Symmetric key cryptography is also referred to as single-key, or secret-key, cryptography. Private key cryptography is interchangeable with symmetric key cryptography and bypasses the problems associated with public key cryptography. Private keys can be used in conjunction with public keys, whereby the sender's private key initially encrypts a message, which is then encrypted again using the receiver's public key. This way both confidentiality and non-repudiation are maintained during a public key exchange.

Asymmetric Key Cryptography

Asymmetric key cryptography is often called public key cryptography because messages are encrypted using a shared public key and decrypted only by a single, unshared private key. Both methods implement the concept of a one-way function.

A sub-set of asymmetric cryptography is Public Key Cryptography. All public-key systems are asymmetric, but not all asymmetric systems are public-key systems.

Public key cryptography (encryption and signing) involves the use of a publicly-shared key, but may or may not rely on an unshared private key. Public key cryptography is almost synonymous with asymmetric cryptography; some public key algorithms do not use private keys. Public key methods require secure separate channels for sending both the message and the key to the designated party and provide no form of non-repudiation, since both sender and recipient use the same key.

Message authentication

Message authentication algorithms involve two aspects of a good cryptosystem: authenticity and integrity. Algorithms designed to verify both authenticity and integrity establish the original authorship for a given message and that it arrives intact and unmodified from its original state. Message authentication schemes take in a secret key and an arbitrary-length message and produce a message authentication code, which protects both aspects.

Digital signatures

Digital signature frameworks serve two distinct purposes:

- Digitally-signed messages assure original authorship upon arrival to the intended party and enforce non-repudiation in the process
- Digital signatures also assure the validity of a message's content upon delivery

Algorithms built to use digital signatures rely on both public key cryptography and hashing functions.

The basic functionality of hash/crypto algorithms (DES, RSA, SHA, MD5, HMAC, DSA), and effects of key length

Hash functions digest messages of virtually any length to provide a unique value derived from the original content of a message, which is known as a message digest. Creation of a message digest then enables the sender and recipient to verify whether or not a message's content has been altered en route to its destination.

Data Encryption Standard (DES) is a symmetric encryption algorithm that operates on 64-bit blocks of data with a 64-bit key (56 bits key, 8 bits parity). Each block mode influences how and when plaintext portions become encrypted. DES is capable of operating in several such modes, including: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB).

Message Digest 5 (MD5) is the industrial-strength message digest algorithm employed by many software integrity and verification software components. MD5 processes 512-bit blocks of data, using four distinct rounds of computation, to produce a 128-bit value with the same padding requirements as MD4. MD5 provides additional security features to reduce the speed and effectiveness of reproducing MD5 results, although it is proven to be susceptible to collisions.

Public key cryptosystems were first widely popularized by Ronald Rivest, Adi Shamir and Leonard Adleman, the original authors of the RSA algorithm. The formation of a commercial venture named RSA Security brought this technology into the mainstream security infrastructure scene.

RSA Security outlines five basic requirements for cryptographic hash functions:

- The input can be of any length
- The output has a fixed length
- The hash function is relatively easy to compute for any input
- The hash function is one-way
- The hash function is collision-free

Secure Hash Algorithm (SHA) was born of a federal standards proposal called the Digital Signal Standard (DSS), originally intended for federal departments and agencies. SHA produces a 160-bit message digest output, which is then fed through a Digital Signature Algorithm (DSA).

One of its latest successors, SHA-384, is capable of producing 512-bit messages with 256 bits of protection against collision attacks.

The **Digital Signature Algorithm (DSA)** uses the asymmetric cryptography standard used to produce digital signatures in the form of long numeric values. These values are composed to verify the author of a message and that the message arrives unaltered.

A **Hashed Message Authentication Code (HMAC)** algorithm ensures the integrity of a message during transmission using a partial digital signature, but lacks non-repudiation. HMAC can be used in combination with other message digest algorithms using a shared key that is distributed only to participating parties.

Key length and security impact

The most critical configuration parameter for a cryptographic key system is in the length of the key itself. A short key choice protecting highly-confidential information drastically reduces the effectiveness of any cryptosystem, regardless of algorithm or implementation. An easily guessed password is easily identifiable to automated dictionary attacks given adequate time and resources. Perhaps the most crucial fact to keep in mind is that a keyspace and algorithm also rely on strong password choice, because even the best implementation is useless against an easily-guessed password.

Part of the strength of an algorithm by which encrypted information is processed is derived from its keyspace; that is, how many bits are involved with key generation. A large keyspace creates computational challenges and raises the bar for a potential attacker. Therefore, it is imperative to utilize algorithms internally designed with an appropriate amount of keyspace for the data being protected. Small keyspaces are the reason many consumer-grade WEP implementations are easily broken by analyzing a few hours worth of captured traffic.

An encryption method's strength, or work factor, is derived from the properties of its algorithm, key length, initialization vectors and the implementation that combines them all. Weakness comes from an implementation or algorithm being vulnerable to feasible computational attack or brute force key recovery.

Key management

Key management requires a well-defined policy for the creation, issuance, storage, distribution, revocation and eventual destruction of company-defined keys. Furthermore, allowances for key recovery must also be made in the event a designated key holder is removed from the organization or is no longer available or cooperative, or when a key or keys become corrupted.

Rules and procedures for secure key management include:

- Keys are never to be kept in plain view nor in plaintext format;
- Keys are to be stored securely and separately from the data they safeguard;
- Key length proportionate to the sensitivity of cryptographically secure data;
- Key randomization to ensure resilience to brute force methodologies;
- Key limited lifetime availability to avoid later replay or reuse attacks;
- Key expiration based on frequency of use;
- Key escrow or back-up services for emergency-use only;
- Secure storage and transmission of managed keys; and
- Secure revocation and deletion of keys when no longer viable

Key distribution methods and algorithms

Proper key distribution is necessary to maintain the integrity of a cryptosystem, its users and the data it protects. Ideally, the mechanisms derived from encryption methods should operate with transparency; that is, the end-user should never be concerned, involved, nor aware of the underlying components involved with key management.

Manual key distribution imparts responsibility on behalf of the key recipient to ensure proper handling, storage and usage, and must be carefully protected en route. Two such architectures that handle industrial-strength key management are Kerberos and ISAKMP.

Ticket-based transaction systems, such as Kerberos, take on a fair amount of this responsibility when storing, distributing or maintaining cryptographic keys or sessions. A Key Distribution Center (KDC) is the primary caretaker for this purpose, establishing a means to provide automatic key distribution.

Internet Security Association and Key Management Protocol (ISAKMP) is a cryptographic protocol that serves as the basis for Internet Key Exchange (IKE) protocols implemented in IPSec. This authentication and key exchange architecture provides the IPSec framework with the missing ingredients it requires: algorithms, protocols, modes and keys for cryptographic exchange between partners.

Error detecting features

Error detection is essential to modern computing technologies especially in the highly-sensitive field of securing and maintaining privacy through cryptographic methods. A subtle error during the creation or conversion of information from plaintext to ciphertext renders the product useless, since the information will not decrypt to its original form.

Key escrow and key recovery

A key escrow is a system of checks and balances that ensures no abuse of personal rights to privacy are violated in cases where law enforcement must obtain access to cryptographically protected information. Separate escrow agencies maintain complementary portions of each key so that no single entity may possess a complete (therefore usable) key. Only a third-party law enforcement agent, operating under a court order, may intervene to recover a full key in the pursuit of criminal evidence or activity.

Of course, not all keys are kept in escrow for purposes of pursuing criminal offenses: keys are also backed-up to ensure that, in the event a key owner is withdrawn from an organization for any reason, the key may be recovered to unlock the information that individual held privately on company resources.

Vulnerabilities to cryptographic functions:

Attacks against cryptographic functions and systems come in many forms derived from two top-level categories: active and passive. An active attack alters key information on-disk, en route or otherwise actively targets an application or protocol weakness. Impersonating an individual, service or server during the exchange of encrypted sensitive information as a man-in-the-middle attack exemplifies an active attack. During a passive attack no activity takes place other than simple observation or reconnaissance: eavesdropping, traffic monitoring and packet capturing are all instances of passive attacks.

The cryptosystems themselves make guarantees for data availability or reliability as they are concerned with the infrastructure. File-at-a-time encryption offers no transparency to the end-user and is rife with the potential to leave unencrypted file contents within the hardware resources, either on-disk or in memory. Holistic drive encryption schemes are better suited to protecting entire volumes in a complete and comprehensive manner.

Attack methods

Active attacks (online) made against a publicly-accessible cryptosystem are generally detectable: brute force attempts against a specific algorithm or component tend to leave evidence in system logs and audit facilities. Passive offline attacks are not quite as obvious, unless an attacker obtained sensitive information (encrypted password files or confidential data) through an obvious channel, such as a deliberate break-in attempt.

However, sensitive data can also be obtained through channels that may not provide adequate audit trails, such as an unfiltered query against a database or Web server, the vulnerability of which may or may not be known, identified or published. There also exists the possibility that an attacker has control over an upstream routing device that facilitates sniffer-based attacks against cryptosystems (such as collecting WEP data or analyzing SSL sessions) that occur completely transparent to the victim and network.

Some of the identifiable attacks against cryptography and cryptosystems include:

- **Brute force** – a systematic approach to key discovery through dictionary-based or algorithm generated password variation.
- **Birthday attack** – digitally signed content is substituted for different data that produces the same digital signature; the name is derived from the notion that there is a 50% chance, in a room of 23 people, that two will have the same birthday.
- **Ciphertext attack** – an attacker attempts to derive the key using several ciphertext samples from the same encryption algorithm.
- **Collision** – the result of two completely different sets of data producing the same cryptographic hash result. This type of attack is interchangeable with a birthday attack.
- **Plaintext attack** – an attacker attempts to derive the key using several portions of plaintext and ciphertext through cryptanalysis.
- **Replay attack** – recorded traffic sent between a targeted client and server link are modified and reissued to the network at a later time. Addresses and time-sensitive parameters are modified to an attacker's advantage.
- **Side-channel attack** – this approach takes into account sensitive timings, observations and principles outside of the encryption algorithm or implementation. Observing the timing differential between reporting back bad information from good information may reveal a methodology for deriving the key, for example.

Certificate Authorities (CAs) and Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) is comprised of software components, formats, protocols, procedures and policies that enable a variety of users and user-specific configurations to communicate in a safe and secure fashion. PKI is a standardized authentication framework based on X.509 protocols and is combined with encryption protocols and algorithms to provide confidentiality, integrity and authenticity.

Certificate Authorities (CA) are organizations entrusted to hold and issue digital certificates once a requesting identity is verified through a Registration Authority (RA). A CA then creates, signs and delivers a certificate to the intended recipient.

Certificates are integral to the PKI since it associates a public key with the properties and components necessary to verify the authenticity of ownership. Every certificate is serialized within the CA and is then bound to the rightful owner. Certificates of this nature are comprised of serial and version numbers, identification, encryption algorithm, expiration date and the signature of the issuing authority.

There are four primary types of certificate, and they are:

- Personal certificates – to identify an individual entity
- Server certificates – to identify the server in a secure exchange

- Publisher certificates – to identify trusted sources of information
- Certificate Authority certificates – divided into root and intermediate roles to establish secure channels between certified individuals, servers and publishers.

Root certificates are self-signed, meaning the subject also doubles as the signer of a certificate, and this type has the ability to issue certificates to intermediates. An intermediate can then assign certificates to individuals, servers, software publishers and other intermediaries

PKI provides confidentiality, access control, integrity, authentication and non-repudiation for participants in a cryptographic exchange.

A PKI consists of the following components:

- Certificate Authority (CA);
- Registration Authority (RA);
- Certificate repository;
- Certificate revocation system;
- Key backup and recovery system;
- Automatic key update;
- Timestamping mechanisms; and
- Client software.

System architecture requirements for implementing cryptographic functions

Application-specific information systems derived for the purpose of secure cryptographic transactions must follow strict adherence to security criteria and evaluation principles. Assessing the strengths and weaknesses of a given system or infrastructure is necessary to ensure the integrity, confidentiality and viability of that system, as it applies to the greater cryptographically secure paradigm.

A handful of the more prominent security evaluation paradigms follow.

The Rainbow Series evaluation is a color-coded classification of security evaluation, assessment and verification methodologies for describing the security disposition. This set of security practices is the product of a DoD initiative to standardize minimum mandated security requirements for information technology.

Classification Criteria

Trusted Computer System Evaluation Criteria (TCSEC) is a combination of functionality and security grading divided into four categories:

- Category A – verified protection
- Category B – mandatory protection
- Category C – discretionary protection
- Category D – minimal protection

Each of these categories classifies computer systems according to the criteria they meet at each level. Information Technology Security Evaluation Criteria (ITSEC) is a security criteria evaluation initiative throughout Europe and provides guidelines by which to assess and measure the functionality and assurance rating for a given computer system or systems. The functionality aspect measures both utility value for the end-user, and tests how well a system performs according to its original design goals and purpose. Common Criteria is a joint TCSEC and ITSEC effort to create a definitive universal assessment of security measures and best practices. Products evaluated by the CC do not guarantee that a given architecture is invulnerable to attack, simply that they meet a minimum level of acceptable resistance to certain classes, categories and methods of attack in a universally recognizable way.

Another evaluation approach for organizations that require strong cryptosystems is through certification and accreditation. Certification assesses a security product as it applies to the principles of security standards. Accreditation is the analysis and reporting phase that documents the details discovered during the certification and testing portions of the evaluation process.

Secure Protocols

Encryption protocols not only for secure static information (in the form of documents and binaries) but also for real-time exchanges between online (or networked) entities. From encrypting individual messages to securing an entire exchange between private parties, these protocols ensure the canons of strong cryptography for Internet transactions.

They include:

- **Secure Multipurpose Mail Extensions (S/MIME)** provides x.509 digital certificate authentication and ensures privacy through the use of Public Key Cryptography Standard (PKCS) encryption for both signed and enveloped messages.
- **Secure Electronic Transaction (SET)** provides a cryptographic protocol infrastructure for the safe transmission of encrypted credit card information via the Internet.
- **Privacy Enhanced Mail (PEM)**, like MOSS, also provides authenticity, confidentiality, integrity and non-repudiation for e-mail messages using X.509 certificates in addition to RSA and DES encryption methods.
- **Secure Hypertext Transfer Protocol (S-HTTP)** provides an additional layer of security for Internet-based transactions by providing cryptographic method negotiation and exchange on a message-by-message basis.
- **Secure Sockets Layer (SSL)** also protects a communications channel (instead of individual messages) for the duration of an exchange using public key encryption.

Other methods are described later in the Data Communications domain.

The application of hardware components, such as smart cards, tokens

Access control mechanisms are based on a variety of authentication tokens, cards and properties that provide several layers of protection against unauthorized access. Physical means include biometric scanners, security badges and electronic keyfobs.

Smart cards take on the appearance of credit cards or security badges that use either a magnetic strip, barcode or integrated circuit which contains information specific to the card holder. Smart cards are physical credentials used to authenticate an individual.

A token is a separate object associated with another resource that describes security attributes and is used to convey information about the subject. Together with smart cards and other forms of authentication credentials, tokens serve to create multi-factor authentication schemes.

IPSEC

IPSec provides the complete infrastructure for creating a cryptosystem, but lacks a few essential ingredients to make it a complete framework. ISAKMP provides the background support and services necessary for the IPSec infrastructure.

IPSec is predicated upon security associations and has four main components:






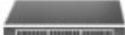

- **Authentication Headers (AH)** to assure integrity and non-repudiation;
- **Encapsulating Security Payload (ESP)** to provide confidentiality;
- **IP Payload Compression (IPcomp)** for improved performance; and
- **Internet Key Exchange (IKE)** for secure key exchanges between parties.

According to RFC2408, ISAKMP requires only four distinct properties:

- Peer authentication mechanisms;
- Security Association (SA) enrollment and management;
- Key generation mechanisms; and
- Protection against replay and DoS attacks.

Data Communications

The Data Communications domain encompasses all manner of network and telecommunications equipment, protocols and components that control the exchange of information between computers. A security practitioner requires a firm understanding of the underlying frameworks and infrastructure that define computer networks to properly secure them against hostile agents, software and activity.

OSI Layer Name	Description	Protocols	Devices
7. Application	The Applications interface for networked communications.	SMB, HTTP, SMTP FTP, SNMP, WWW Telnet, AppleTalk	
6. Presentation	Responsible for encryption and data presentation.	HTTP, FTP, Telnet, SMTP, AFP, TDI, GIF, MPEG, JPG	
5. Session	Creates a connection between two endpoints and establishes an "end-to-end" bidirectional channel of communication.	NetBEUI, SPX, RPC, TCP, UDP (Port Numbering)	
4. Transport	Ensures the integrity of data sent between two locations.	IPX, UDP, NWLink, TCP, SPX, NetBEUI	
3. Network	Addresses logical locations.	IP, IPX, NWLink, NetBEUI	
2. Data Link	Encapsulates data into frames.	Ethernet, PPP, HDLC	
1. Physical	Physically moves the data over a hard wired line.	Ethernet, Token Ring, FDDI	

Network security takes a multi-layered approach to be truly effective against unruly end-users, malicious automata and all manner of malware. Security protocols, mechanisms and frameworks are implemented from the physical media transmitting electrical signals to the user applications utilizing those media. International Standards Organization/ Open Systems Interconnection (ISO/OSI) Layers and Characteristics

The International Standards Organization (ISO) is one of two main telecommunications and network standards organizations. The Open Systems Interconnect (OSI) is a global federation designed to specify and model international standards governing open network architectures. One of the most prominent bodies of work produced by the OSI is the TCP/IP reference model described in the seven layers below.

Physical Layer

The first layer, the physical layer, describes the media, signaling, line voltage and bit conversion implemented in end-to-end and point-to-point equipment. Network interface cards and twisted-pair cabling specifications are examples of physical layer properties.

Data Link Layer

Layer two is called the Data Link Layer (DLL) and is where information from the upper layers gets formatted into the proper representation for the physical layer. ARP and Reverse ARP (RARP), and Point-to-Point (PPP) protocols occur at this level.

Network Layer

Inter-network services, protocols, addresses and routing schemes occur at the third layer of the OSI reference model. Common protocols at this layer are IP, ICMP, IGMP, RIP and OSPF.

Transport Layer

Reliability and serialization are implemented at the fourth level, the transport layer. End-to-end transmissions are treated to a variety of data stream partitioning and reassembly, integrity checking, recovery of lost packets and flow control. TCP and UDP are commonly found at this layer.

Session Layer

Layer five, the session layer, is concerned primarily with the construction and destruction of communications channels and the interconnection between applications. Dialog control, negotiation and maintenance of sessions are handled at this layer by NFS, SQL and RPC protocols.

Presentation Layer

As the name implies, layer six is concerned with the presentation of data as used by the uppermost layer. Translation from lower level data into standard usable formats such as textual data (ASCII, EBCDIC), visual imagery (TIFF, JPEG) and multimedia formats (MPEG, MIDI) occurs in this layer.

Application

Layer seven is where user interaction with network applications takes place. File and mail transfer applications, Web browsers and peer-to-peer file sharing programs are examples of application-level properties. Communications and network security

Securing communications against all possible forms of attack is a never-ending task. Security protocols occur at every layer of the OSI reference model, from the physical layer to the application layer, and vary

widely from one application to the next. Security policy extends from the physical layer to the application layer, and continues beyond the OSI reference model to cover the people implementing, operating and/or maintaining large networks of computers.

Physical media characteristics define the type of equipment that can be used for a given network environment. A few of the more common network technologies in use today include fiber optics, coaxial cable and Shielded or Unshielded Twisted Pair (STP/UTP).

Fiber optics cabling utilizes a glass-based core wrapped in a protective cladding and sleeved in a second protective outer jacket. Being glass-based, fiber optics is capable of achieving much higher bandwidth over longer distances than ordinary copper-based products. Furthermore, fiber optics is immune to signal attenuation and electronic noise.

Common coaxial cabling begins with a copper core surrounded by a braided shielding layer and grounding wire enclosed within a durable protective jacket. Coaxial cabling provides fair resistance to EMI and excellent bandwidth potential. Typical LAN configurations may use 50-ohm cable for digital-only signaling, or 75-ohm cable for combined analog/digital signaling. Compatible equipment is capable of transmitting and receiving baseband signals (a single channel at a time) or broadband (several at once).

There are two forms of twisted-pair cabling and both begin with eight individually insulated copper wires sheathed in a protective jacket. This is called an Unshielded Twisted Pair (UTP) cable, unless there is an additional foil shielding, which is then called a Shielded Twisted Pair. The signature twists provide resistance to crosstalk and the inclusion of foil shielding further increases resistance to external interference.

UTP is graded according to build quality and materials, as summarized below:

- Category 1 – common analog (voice) cable
- Category 2 – digital transmission (up to 4Mbps)
- Category 3 – Ethernet/10Mbps or Token Ring/4Mbps
- Category 4 – 16Mbps Token Ring
- Category 5 – 100Base-TX/100Mbps for CDDI and ATM
- Category 6 – 155Mbps high-speed Ethernet links
- Category 7 – 1 Gbps Gigabit Ethernet

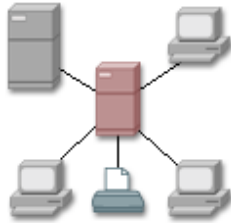
Common networking equipment uses CAT-5, while more modern installations get treated to either CAT-5e (enhanced CAT-5, an incremental improvement to CAT-5) or the increasingly popular CAT-6 and CAT-7 types for high-speed LAN connections.

Network Topologies (e.g., Star/Bus/Ring)

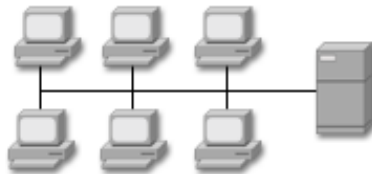
A network topology refers to the manner in which a network is physically connected and identifies the arrangement for a given network of computing devices.

Three of the more common network topologies include:

- **Star** – in this arrangement, all network devices are centrally connected to a hub, switch or router, and extend outward in a fashion similar to the points of a star;



- **Bus** – one cable ties together all computers in a sequential fashion with each node tapping into drop points on the cable; and



- **Ring** – a series of nodes are connected one after another, forming an almost circular, unidirectional circuit path.



Incidentally, each network topology implies the types of applications, protocols, and hardware deployed on a given network.

TCP/IP Protocol Characteristics and Vulnerabilities

The TCP/IP suite is actually a richly-layered protocol stack consisting of dozens of separate protocols, although TCP and IP are most commonly cited and frequently used. TCP/IP itself is platform-independent, based on open standards and is available on nearly every operating system. For better or worse, TCP was designed ultimately for ease-of-use in a time when security was not a heavy concern, and most users more or less behaved. By nature, TCP is overly trusting of the information it receives and passes, opening a Pandora's Box of network-driven attacks.

User Datagram Protocol (UDP) is also frequently deployed on local and wide area networks, and like TCP lacks inherent security mechanisms to ensure verifiable receipt of untainted goods from trusted sources. Transport layer protocols such as TCP and UDP are not the only potential sources of weakness, as network protocols like Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP) are also susceptible to trust-based attacks. Solutions to some of the modern problems conventional TCP/IP protocols encounter are provided in the material further in this chapter.

Local Area Networks (LANs)

The three primary Local Area Network technologies used today are Ethernet, Token Ring and Fiber Distributed Data Interface (FDDI). LAN topologies are self-enclosed networks by nature that extend to several computers on a floor or several floors of computers in a building.

Wide Area Networks (WANs)

Wide Area Network topologies refer to physically distinct networks separated by location or region. WANs are usually connected via packet-switched technologies like X.25, Frame Relay and Asynchronous Transfer Mode (ATM), or through private circuit links such as Point-to-Point Protocol (PPP), Integrated Services Digital Network (ISDN) or Digital Subscriber Line (DSL). WAN technologies are based on long-distance communications links categorized into leased and dedicated designations.

Remote Access/Telecommuting Techniques

A centralized authentication methodology provides the convenience of low administrative overhead and a single point for login credential configuration. The drawback is that centralization also creates a single point of failure, which is essentially an all-or-nothing proposition. Two distinct technologies in this category are Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS).

RADIUS is a centralized login system for remote dial-up clients. RADIUS operates similar to domain clients passing login credentials to a domain controller, and separates the authorization server from the authentication server. This is intended to serve as an additional layer of security against remote authentication attacks. TACACS is an alternative remote authentication mechanism to RADIUS that works along the same principles of centralized authentication.

Internet/Intranet/Extranet

The Internet is a global fabric of intricately woven networks that combine to create what is known simply as the Web. Globally accessible services, applications and servers are interconnected through a variety of mixed networking technologies creating a vast wealth of on-demand resources.

Intranet architectures use, primarily, Internet-born technologies in a localized context. Web, FTP and mail services commonly occur within well-defined network boundaries exclusive to the outside world. Think of intranets as smaller privatized instances of the Internet, designed specifically for a particular organization to centralize internal data.

Extranet topologies enable two or more intranets to communicate and share otherwise localized services, resources and applications. Business-to-business operations may require collaborative partnerships between intranet resources to accomplish a common goal, such as joint project development or sharing catalogs and database information.

Firewalls

Firewalls are packaged in many forms, with varying types of capability, but all of them service a common goal: to restrict access between separate network entities. Typically this means logically separating a corporate network from the Internet, and policing the interaction between both. Packet filtering, stateful inspection and application proxies represent some of the primary capacities and layers in which a firewall operates.

Routers

Routers route traffic between separate network topologies. Network layer protocols (layer 3) such as IP, ICMP, TCP and UDP are commonly implemented in routers. A router may be a stand-alone device with a partial network stack, or full-fledged bank of computers running desktop and server applications.

Switches

Switches generally switch packet frames at the data link layer, except in the case of a layer-3 switch. A switch only directs traffic to and from the appropriate network interfaces on a shared medium, between local devices (computers, hubs and other switches).

Gateways

A gateway device bridges different connection media and translates, or restricts, the ability for endpoints to communicate. Gateways operate at the data link layer to translate FDDI to Ethernet frames, at the network layer translating between incompatible protocols like IPX and IPv4 and at the presentation layer when exchanging different mail formats.

Proxies

Proxies come in many shapes and sizes, but they most commonly serve as go-betweens for internal client computers and external resources. Content filtering may or may not occur on a proxy, and the proxy can be limited to passing only certain protocols or specific types of traffic and content. There are proxies that operate on multiple layers, from ARP proxies at the data link layer, to upper-level protocol interfaces in the form of application, circuit and kernel-level proxies.

Protocols

Protocols are the lingua franca of network communications implemented in protocol stacks on network-capable devices. A protocol defines the rules and restrictions that govern how data is formatted, transmitted and presented between interconnected end-points. In network-based communications media, a protocol specification outlines the entire framework of protocols, properties and parameters that make up the network architecture, the most popular of which happens to be the TCP/IP protocol suite.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Transmission Control Protocol/Internet Protocol (TCP/IP) is the de facto standard for inter-network communication. Although the TCP/IP framework actually consists of many other protocols these two (TCP and IP) are the most prominent components, as they are integral to the most basic and common network operations. IP is primarily focused with inter-network addressing and packet routing, with the ability to handle fragmentation and reassembly where necessary. TCP is a serialized connection-oriented protocol to establish state-based communication between two points to ensure reliable delivery.

Network Layer Security Protocols (IPSEC, SKIP, SWIPE)

Securing protocols based on IP specifications is accomplished through strong, verifiable frameworks that enable sender and recipient to authenticate, validate and safely transmit sensitive information across the Internet.

Primary examples of IP-related security architectures include:

- **Internet Protocol Security (IPSec)** is a standard architecture that provides a method for establishing secure channels for exchanges between entities. IPSec provides message authentication, access control and non-repudiation for IP-based protocols.
- **Simple Key Management for IP (SKIP)** is an encryption tool designed for securing connection-less protocols, which integrates with IPSec and operates at layer 3 of the OSI reference model.
- **Software IP Encryption (SWIPE)** also operates at layer 3 for IP to provide strong authentication, integrity and confidentiality through encapsulation.

Application Layer Security Protocols

Commonly-used email security solutions are:

- **MIME Object Security Services (MOSS)** provides authenticity, confidentiality, integrity and non-repudiation for e-mail messages using Message Digest 2/5 (MD2/MD5) algorithms, RSA public key encryption and DES for authentication and encryption services.
- **Secure Electronic Transaction (SET)** provides a cryptographic protocol infrastructure for the safe transmission of encrypted credit card information via the Internet.
- **Privacy Enhanced Mail (PEM)**, like MOSS, also provides authenticity, confidentiality, integrity and non-repudiation for e-mail messages using X.509 certificates, in addition to RSA and DES encryption methods.
- **Pretty Good Privacy (PGP)**, though not a standard, is a cryptosystem that promotes secure email transactions through the provision of symmetric and asymmetric key algorithms, message digest algorithms and the necessary core protocols and software components.

CHAP and PAP

Challenge Handshake Authentication Protocol (CHAP) provides security in addition to the PPP login protocol by implementing a challenge/response mechanism. When negotiating a user request, a CHAP server issues a random value called a challenge, which is then encrypted with a predefined key by the client, and then returned to the server. The server then creates its own encrypted version using that same key and compares it against the client key.

Password Authentication Protocol (PAP) is a protocol that provides remote user identification and authentication via PPP connections. PAP transmits login credentials, in cleartext across the wire, exposing private information to packet sniffing attacks.

Carrier Network Services

High-Level Data Link Control (HDLC) operates on layer 2 of the OSI reference model and is itself an ISO standard for data transmission across synchronous lines. HDLC supports full-duplex communications with flow control and error correction for both point-to-point and multi-point connections.

Frame relay is a data link layer protocol based on packet-switching technology that enables multiple companies and networks to divide a common communications medium.

Synchronous Data Link Control (SDLC) is a bit-oriented layer 2 protocol originally developed by IBM for remote communication with SNA servers over leased or dedicated lines.

Integrated Services Digital Network (ISDN) is, as the name implies, a digital end-to-end high-speed communications framework designed to integrate with existing voice network infrastructure equipment.

X.25 is an older WAN packet-switching data communication standard designed to use virtual circuits between point-to-point connections over a shared connection medium. X.25 is a cumbersome protocol that operates at speeds comparably slower than frame relay and ATM networks.

Communications security

The TCP/IP suite has some error prevention, detection and correction capability built right into the framework itself. Some applications and configurations require assurances above and beyond that native framework, which is why a plethora of security protocols, mechanisms and components exist to fortify network devices and communications against attack.

Network encryption protocols and strong authentication schemes are necessary to maintain the confidentiality, integrity and authenticity of network-based transactions. Encryption can occur at one or more levels, and in combination, to provide varying levels of resistance to the various methods of cryptographic attack.

Tunneling

A firm basis of understanding in the concept of tunneling and tunnel protocols is required to grasp the nature, form and function of Virtual Private Network (VPN) solutions. Tunneling is a process of encapsulating the contents of one protocol into another, presumably more secure protocol. By enclosing one protocol within another, the concept of tunneling is achieved by creating a virtual pathway between beginning and end-points of a communications link.

Virtual Private Network (VPN)

VPN technologies are designed to encompass a broad range of security mechanisms, encryption algorithms and network protocols to serve a single common purpose: establish a secure Internet communication path between sender and receiver, where both are established on private, internal networks. This can be a one-to-one or one-to-many relationship, involving a number of LAN and WAN network technologies, from remote access dial-up or broadband connections, to IPSec and SSL/TLS encryption capabilities.

There are primarily four common VPN protocols:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer-2 Tunneling Protocol (L2TP)
- Internet Protocol Security (IPSec)
- Secure Socket Layer/Secure Transport Layer Security (SSL/TLS)

Each of these implementations has their own unique set of requirements, advantages and distinctions. Contemporary SSL/TLS-based solutions, such as the OpenVPN specification, represent a modern twist on the concept of VPN security, offering a more simplified, portable and flexible solution than the more intrusive IPSec-type solutions.

Network Monitors and Packet Sniffers

Network analyzers, protocol analyzers and packet sniffers are all essentially describing the same technology. These diagnostic tools are a double-edged sword for security practitioners, for they not only enable administrators to observe network interactions, but in the hands of an attacker, can be used to eavesdrop on private communications.

Most network and protocol analyzers are designed with a diagnostic purpose in mind, while some packet sniffers are specialized applications used to distinguish, dissect and decode vulnerable data streams. The true distinction between good and bad is in the intent of the person observing network traffic with the protocol analyzer.

Network Address Translation (NAT)

Network Address Translation, or NAT, is a method of masquerading one generally-accessible host as several interconnecting, remotely-inaccessible client machines. NAT is most commonly used in many consumer-grade router solutions as a means to provide Internet access to many client computers through a single service subscription. However, the original intent behind the NAT design is to address the decreasing availability of IPv4 address space.

E-mail security

The Internet architecture operates largely upon the Simple Mail Transfer Protocol (SMTP), which by itself is barren of any security mechanisms. Eavesdropping attacks can be performed at several points on the network, from snooping on the wire to prying into mail server spools and repositories for plaintext messages. To that end, encryption-based solutions such as Secure Multipurpose Mail Extensions (S/MIME) were created to establish a means to electronically sign messages using public keys and digitally verify these signatures upon receipt.

Some of the goals of email security include:

- Provision for non-repudiation of messages;
- Restricted access to messages and attachments;
- Verifiable message integrity and delivery; and
- Content sensitivity classification within messages and attachments.

For more information, refer back to the Application Layer Security Protocols sub-section under the Data Communications domain heading.

Security boundaries and how to translate security policy to controls

Security boundaries are defined by the devices, protocols and user interactions that are permitted to occur on the network. For example, users located in the research and development department of an organization have no business tooling around the computers in accounting, so a boundary is defined to separate the interactions, permissions and actions that developers may take against accounting resources.

In the same way, network transactions, protocols and processes comprise a greater overall security policy that defines the events and activity that are permissible. Knowing how each user, process and application interacts with other systems, devices and entities is instrumental to understanding how to define security policy for those interactions.

Network Attacks and Countermeasures

Methods of network-based attack are discussed earlier in the Access Controls domain. There are many avenues of approach an attacker may take on his or her journey through a remote network, so no device should be left out of the security equation.

ARP

ARP attacks are applied locally to IP and WiFi networks to assume the role of intermediate routing devices and end-points, either to perform Man-in-the-Middle attacks or connection hijacking. ARP cache poisoning is one example of this kind of attack. Maintaining constant vigil and a static ARP cache is the best countermeasure against various forms of ARP attack.

Brute force

First and foremost, enforcing password and passphrase best practices is the best preventative maintenance against brute force attempts made against authentication schemes. Users should be informed on how to select strong entries that are not easily guessed by automated attacks. Public-facing authentication mechanisms thorough accounting of failed login attempts and specified attempt thresholds should be set in place to stifle brute force automata.

Worms

Worms spread quickly, efficiently and easily, especially when unhindered by protective network and host-based preventive applications. While some worms focus on an identified weakness on a targeted platform, others simply arrive through normal channels, only to become invoked internally by an unsuspecting end-user. Constant upkeep to platform and application patches, staying abreast of security bulletins and real-time or regularly-scheduled malware scanning routines are some of the best preventive maintenance against worm infestations.

Flooding

Flooding is the malicious act of inundating a server or its services with an overwhelming amount of data, to the point where the system either continues to operate without service to new incoming connections or shuts down completely.

Protection at the border of a network, using firewall and perimeter device Access Control Lists (ACL), can help reduce the effectiveness of flooding attacks. Placing restrictions on the number of incoming connections permitted within a given window of time protects against any surge in inbound connections, while local user and process restrictions on the operating system control user and application behavior.

Eavesdropping

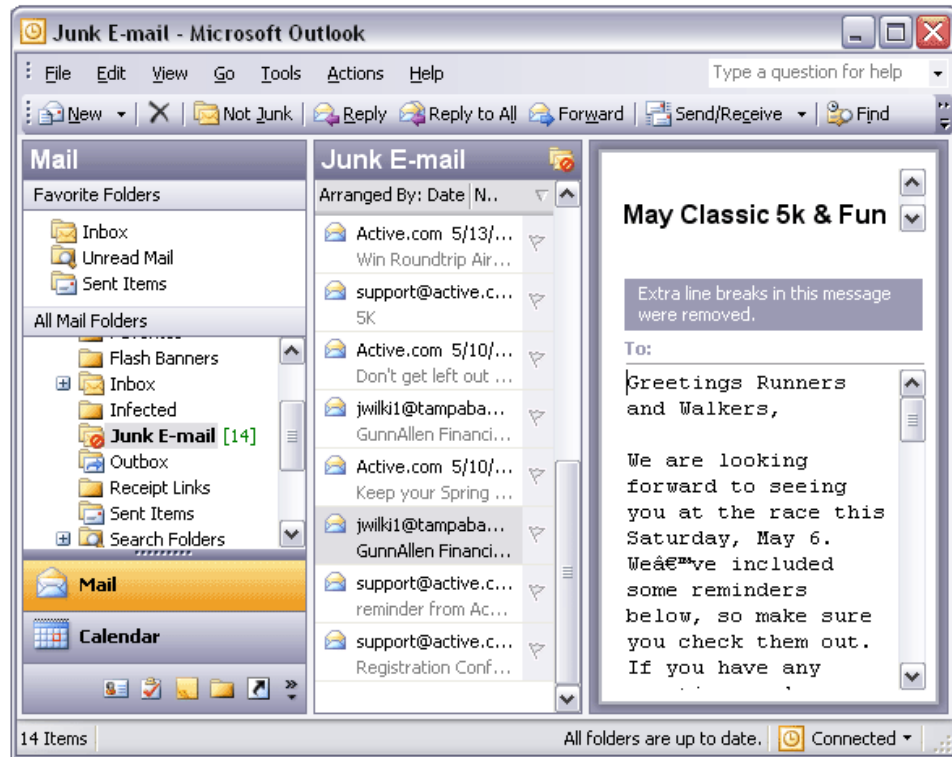
An eavesdropping attack is predicated upon an ability to intercept and interpret communications, whether transmitted by voice or by signal. Restricting direct access to physical network resources and governing the involvement of network-based transactions, while maintaining tight control over unauthorized or unapproved devices attached to the network, is a good start.

Refer to the end of the Auditing and Monitoring domain for information regarding eavesdropping attacks.

Sniffers

Sniffer-based attacks require advanced preparation and administrative access to network resources. Network analyzers used to diagnose traffic problems are capable of intercepting and interpreting many types of protocols, some of which leave otherwise confidential information exposed to eavesdropping. The best practices to use to combat the effectiveness of sniffing attacks are to use strong authentication schemes between client/server services and encryption protocols where applicable.

Spamming



Spam is best handled at the ingress point, where mail is received and processed, before it is permitted to propagate to end-recipients. Known-bad blacklists, content filters and malware scanners are a few methods that can be utilized to sanitize incoming messages with varying degrees of success. Also, you should maintain constant watch over mail server activity, and follow-up on invalid logins or apparent break-in attempts to avoid enabling a spammer to turn a company server into a relay point.

Malicious Code

Malicious code objects encompass a wide variety of programmed security threats that seek to exploit various layers and levels of computer vulnerability, from the network to the operating system, to applications running on a remotely targeted operating system. Certain hostile objects are designed to replicate on a single machine or spread across many, whereas others are single-shot attacks aimed at crippling security measures or significantly compromising them to enable unauthorized access. Worms, Trojan horses, viruses and compiled or scripted exploit code (in its various forms) are all included under this umbrella terminology.

Where some instances of malicious code usage are the result of targeted vulnerability exploitation at the hands of a cracker, other instances involve many automated agents working together against one or many targets, such as Distributed Denial of Service (DDoS) tools and worms. Then there are the many forms and functions of scripted client and server-side attacks, distributed attachment payloads and a multitude of hostile executable code examples.

Malicious code concepts

Several recurring concepts regarding malicious code make up the general hierarchy into which malicious code is categorized. These concepts are explained and explored further in the following text. Some concepts, such as viruses and worms, are well-established and have flourished for decades, whereas ActiveX components and Java exploitation methods are much newer to the security scene.

Definitions

Malicious code is a well-defined classification of concepts and components described entirely in its own taxonomy. Each descriptive term distinguishes a class and type of malicious code component from Polymorphism, in computer science, is the ability for code to mutate into a new form producing a new signature, while keeping the original algorithm intact. This produces a new signature and assists code (viruses, exploits and worms) in remaining hidden from scanning agents. Polymorphic code is usually achieved through the use of run-time decryption routines.

Stealth viruses attempt to conceal themselves from discovery by anti-virus applications through hooking system functions used to read files to infect files on-the-fly. At run-time, a stealth virus forges the results to applications that call upon the infected form, so that a clean, uninfected file is read.

Heuristics is a method of detecting previously unknown (or unidentified) foreign objects as potentially hostile code streams. The methods for employing heuristics are vast and varied, but they all essentially work on the same principles: check foreign code attributes for virus-like characteristics without the assistance of virus signatures or definitions. Heuristics establishes a baseline for acceptable behavior on a host computer, and uses that baseline as a reference to detect abnormal activities and events.

Malware is another all-encompassing term that is comprised of malicious code elements ranging from viruses and worms, to spyware and adware. In legal circumstances, malware is sometimes called a computer contaminant, according to the laws governing several U.S. States. Malware is not considered applicable to software components or coding constructs that are merely flawed or broken in some way with no identifiable malicious intent.

Behaviors

Software generally conforms to expected and acceptable forms of behavior: a word processor, for example, should never wipe a hard drive clean under any circumstances, and a graphics editing application has no business poking around in the boot sector. There is a baseline of behavior by which known and unknown applications should operate, and using expert technology, a malware detection engine can determine untoward application behavior using the baseline as a reference point.

Behavior-based or statistical engines are designed to detect anomalies in system behavior at both the network and operating system levels. Intrusion Detection Systems (IDS) safeguard against network-born anomalies whereas heuristics-based anti-virus engines detect behavioral anomalies occurring within an operating system.

Jargon

Jargon in this context is the technical slang used to describe and express informal ideas or concepts specific to computer culture. Unlike standard terminology, this commonly accepted form of expression is particular to computer-related technology that is confusing to the uninitiated. Several basic examples of ordinary computer jargon are described briefly below.

Myths/hoaxes

The category of myths and hoaxes is defined, developed and distributed by individuals motivated to spread fear, uncertainty and doubt for purposes of entertainment, or to give a negative impression to an organization, group or software product. While no physical damage takes place in the wake of a major hoax or mythical all-destructive virus, considerable time, resources and attention are wasted on researching, reacting and responding to the problem in a timely and corrective manner.

Hackers, crackers, phreaks, and virus writers

One distinction that can be made between hackers and crackers is that of motivation: while a hacker is capable of circumventing security mechanisms, or successfully exploiting software vulnerabilities, a cracker is committed to these acts in a purely criminal context. Both groups target computer systems and derived platforms or software applications. Phreaks or phreakers typically exploit phone systems, which may or may not involve computer system penetration. Virus writers author malware for the express purpose of infecting a target system and replicating locally despite any anti-virus coverage on that machine.

Denial of service

Denial of Service (DoS) attacks also arrive in many forms, but the intent is generally the same: to deny service of some target application, computer or network to their respective clients. DoS vulnerabilities represent the breadth of weaknesses in a target architecture or application that do not yield access to protected systems and resources. This can be a simple attack against a corporate Cisco IP phone that renders it inoperable, triggering an application to crash without recovery, or a distributed attempt to saturate a targeted entity's server resources so they are inaccessible to all.

Computer viruses and other forms of malicious code

Computer viruses are a long-standing threat to computer security and continue to pose a threat even with several years of technological advancement. With that advancement also come more advanced forms of malicious code, including the once impossible task of creating malware vectors within simple office documents. Viruses are described by several well-accepted categorical imperatives described below.

Various types of computer viruses

The nomenclature applied to a given virus is defined by the native functionality it provides. Where it infects, and how it replicates, are important characteristics in determining the type of virus.

Multi-partite, or multi-part viruses, utilize several propagation techniques in a continued attempt to elude system security measures and further penetrate into a target machine. This can occasionally span separate boundaries and combine several characteristics to be recursively infective for each target. A typical example usually implies code that operates both in boot-record infection methods and file infection methods. Macro viruses are driven by templating or scripting engines contained in office productivity software. A macro virus infects and replicates by taking advantage of internal application functionality from within the document.

A boot record infector (or boot sector infector) positions itself at the start of the system boot sector to obtain stealthy control over basic computer operations while resident in memory. From there, an infector may then spread to other drives on the system, including unsecured network-attached drives and storage units.

Worms and viruses are not as common for Macintosh computers, though they do exist for modern OS X installations such as the Ingtana. A worm and the Leap.A, or Oompa-Loompa virus, both created for version 10.4.

Viruses that target specific binaries and executable file formats to inject code functionality that enables delivery or replication upon execution by the host are known as file infector viruses. The propagation routines are relatively unsophisticated as compared to multi-partite or polymorphic viruses, and serve only to create activation points within other applications so that it can spread quickly.

These viruses are easily detectable and sometimes show up in the form of a companion virus, an executable bearing the same name but different extension of a known-good application (for example, a BINARY.EXE target with BINARY.COM infector). As a result, a careless user might accidentally invoke the companion virus executable activating the malicious code completely unnoticed.

Worms

The key distinction between a worm and other forms of malware or malicious code is that worms do not require the intervention, interaction or invocation by an end-user to accomplish its goals. Worms propagate throughout a network by attacking network-accessible resources: applications, protocols or platform vulnerabilities that are left exposed and unprotected. Once a system is conquered, a worm's primary goal is to find other unwitting participants to serve as hosts for one of the quickest spreading infection vectors threatening modern security models.

Trojan horses

While Trojan horses differ greatly in delivery and mechanism, the intent is always the same: get an unwilling participant to activate it into executing the designer's objective. Any software that arrives untested from an unverified source is a major violation of computer security best practices and is the means by which many Trojan horses arrive. A seemingly benign attachment could potentially contain malicious code comprised of functionality that can destroy local data, expose it to the author or yield unrestricted remote access for an external attacker. If left unchecked, a Trojan horse can be the gateway to further penetration or destruction of resources and computers.

Trojan horses can be patched functionality that loads in advance, or in addition, to original binary functionality. They can also be purpose-built programs that replace system-critical binaries, such as authentication schemes or remote login shells, like SSH, to provide unauthorized access to resources or information. Network startup scripts are also a potential target for Trojan horse activity, where an attacker can insert services or shells that persist across reboots, providing reproducible back door access.

Logic bombs

Logic bombs are objects preprogrammed to trigger based on a series or sequence of events, at a specific time or a mixture of these conditions. The intent behind a logic bomb varies as much as the form and function of the logic bomb, from covering tracks at a preset time or under predetermined conditions, or they may disrupt a variety of computers or applications at some specified date and time, as a juvenile prank.

Salami attack

In a salami attack the intent is to make the most of several small criminal acts in the hopes that the larger criminal act goes undetected. A bank clerk that embezzles money by altering accounting software to deposit fractions of a cent of every transaction into an unauthorized bank account is applying a salami methodology to crime.

Software or programming techniques which can be exploited (attacked or compromised)

Active content is comprised of web programs that are downloaded to a client machine and executed locally to provide a wealth of dynamic functionality without burdening the server with processing tasks. In effect, the server offloads both processing chores and the risk of processing potentially hostile code to the client computer, which can pose a significant threat to unsuspecting and unprepared end-users.

ActiveX

ActiveX is a language for building interactive software components for enhanced Web content. ActiveX controls are governed by user-specified security levels and authentication properties, which are configured from within the Web browser. Since ActiveX components are downloaded to the recipient machine, they will execute with far greater access to local resources than components written in Java, which executes in a sandbox.

Java

JavaScript and Java applets are an excellent way to create portable exploitation constructs using seemingly innocuous scripted objects. Java creates intermediate bytecode that can be interpreted by virtually any processor. A Java Virtual Machine (JVM) then converts this intermediate bytecode into processor-specific machine code so that it executes locally in a platform-independent way.

When a Java applet is executed from within a Web browser, it happens entirely in a sandbox that attempts to restrict the ability for a piece of code to violate local security policy. This does not always go according to plan, and occasionally a Java component will provide access to local resources that should otherwise remain off-limits.

Mobile code

Mobile code in a malicious context applies to any object or series of objects obtained from a remote location via a network, and delivered to a local machine or group of machines without the knowledge or permission of the recipient. There are many vectors by which mobile code arrives, from downloaded email attachments or document macros, to executable browser objects like ActiveX, Java and Flash or Shock-wave animations.

Trap doors

Any undocumented command sequence designed to bypass normal security restrictions is considered a trap door component, as it allows presumably unauthorized access to authorized sources. Sometimes they are the result of the software development process to enable developers quick access into a system for debugging purposes, and other times they are inserted by unscrupulous individuals to provide surreptitious reentry.

How malicious code can be introduced into the computing environment

Hostile foreign objects arrive through many channels, leveraging an increasingly wider variety of methods, and ranging from the inept brute force trial-and-error process to the finesse of a well-executed multi-stage attack. Seemingly harmless activity such as browsing a Web page or opening an email attachment can bring about malicious code in a completely transparent manner.

Brute force

Brute force mechanisms can be applied to either local or remote targets often with surprising results. The key to most authentication brute force attempts is to exploit weaknesses derived from human sources, such as poorly chosen passwords, as opposed to attacking the security mechanism itself. For example, a brute force attempt leveraged against the SSH daemon attempts to identify easily-guessable login credentials, instead of exposing weaknesses in the underlying implementation or encryption algorithm.

Other targeted attacks take into consideration the internal implementation and/or algorithms only where known or suspected weaknesses may lead to exploitable conditions.

Wardialing is also considered brute force attack due to the sequential nature by which a wardialer attempts to identify carrier tones. Brute force attacks are generally unsophisticated and quite noticeable, but can yield viable results for an attacker if left unchecked. Brute force attacks are explained in greater detail following the Methods of Attack portion of the Access Controls domain.

Dictionary attacks

Dictionary attacks are the primary basis for a typical brute force attempt against authentication schemes. A dictionary is comprised of compiled word lists of common words, phrases and number-letter-punctuation sequences that make up the bulk of easily-guessable passwords. Dictionaries can be localized to a specific region or type of device (likely router passwords for an ISP in the US versus a home desktop in Korea) and elaborated upon by brute force algorithms that transpose characters or generate combinations and variations of dictionary words.

For more information on brute force and dictionary attacks, refer the sub-heading titled Methods of Attack within the Access Controls domain.

Spoofing

The act of spoofing is a direct violation of trust, usually to disguise the origin point of an attack, or to facilitate the interception or interruption of normal operation. A system cracker may employ spoofing locally to create a fake login prompt or masquerade as another host to sniff traffic on an Ethernet segment, or apply spoofing remotely to obscure the source of a full-fledge packet flood.

In the context of a Man-in-the-Middle (MitM) attack, spoofing can be used to facilitate the insertion of arbitrary data into a download session or inject protocol commands into a connection to wrestle control away from another computer.

Pseudo flaw

A pseudo flaw is any programming or configuration error intentionally placed on a system to lure system crackers in an attempt to observe their behavior and trigger system-wide alerts. As an example, an intentional vulnerability is introduced to an exposed machine called a honeypot to serve as low-hanging fruit that draws attention away from well-guarded, mission-critical machines. When a successful attempt to exploit the pseudo flaw is made, administrators are notified of the intrusion and can isolate the attacker's activity on the network.

Alteration of authorized code

The alteration of authorized code can be in the form of a binary patch that cripples or removes security functionality, or one that modifies the configuration or credentials on the target machine. Either this happens due to exploitation or some infectious agent, or deliberately at the hands of a hostile user. Unsuspecting code may crop up through normal channels (public FTP, company email or removable media), or through an external source with electronic or physical access to internal resources.

Flooding

Flooding is a form of resource exhaustion, either to an operating system platform (e.g. a process saturation attack) or to an application operating on that platform (e.g. a socket saturation attack). Enforce strict policies that specify the frequency and concentration of resources for every user, process and connection, and enable process accounting where applicable.

Spamming

Spamming is an attack directed at overwhelming a Web server with large volumes of unsolicited emails. Content is a mixture of dubious advertisements, bogus offers, ill-advised investment schemes and the occasional malware, but remains a constant and undesirable consumer of system resources. Network and application-layer content filters and scanners are the best first line of defense against spam contaminants.

Cramming

Cramming is an act of fraud committed by unscrupulous third-party providers against telephone service subscribers. Crammers bill customers for fraudulent services neither asked for nor authorized by the subscriber.

Programming techniques that can be exploited

In addition to the plethora of vulnerable code and configuration error exploitation methods, there are many directly malicious code constructs that can potentially violate security measures. Dynamic Web content creation languages and portable applet technologies ensure an almost universal compatibility for a number of common devices, but that same convenience can be advantageous for an attacker as well. The ability for an attacker to write arbitrary data to a desirable location can be as effective under the right circumstances as tricking an application or processor into digesting and directly executing arbitrary code.

ActiveX

ActiveX controls push the burden of responsibility to the end-user to make responsible decisions about activating signed or unsigned and verified or unknown components. Since ActiveX components operate entirely on the client machine, they have greater potential to control or modify application and system behavior.

Java

Although the Java sandbox does a fairly good job of containing bytecode, there is an occasional exposure or vulnerability that leads to code breaking into the host environment. Runtime anti-virus and malware scanners are an excellent line of defense against Java-based malicious code.

Mobile code

Mobile code poses numerous threats in terms of form and function. Not all mobile code can be isolated, since not all mobile code can be identified — as is the case for a user who is victimized over an SSL link to an attacker via the Internet. Where it can be identified, foreign mobile code should be isolated and executed on completely isolated machines, preferably in the network DMZ. Only authorized downloads, installs and extensions should be permitted to ensure an optimal level of security.

Trap doors

Though signed and verified downloads are a great way to ensure integrity of deliverables, it does not account for any real or perceived compromise to integrity performed by the developers. Trap doors sometimes occur as innocuous diagnostic portals into complex software systems for debugging purposes; they can also occur through malicious code insertion. A thorough and proper code review is one of the best means to audit a codebase against internal policy.

Mechanisms that can be used to prevent, detect and correct malicious code and their attacks

In order to maintain control over the increasing variety of malicious code attacks, anti-virus software has expanded from its original virus-scanning capacity to include detection and removal of rootkits, adware and spyware applications, in addition to providing run-time coverage and sandbox emulation of unverified code.

The theories, techniques and technologies employed vary from one vendor's product line to the next, but they all provide coverage against malware-based attacks.

Anti-viral protection

Anti-virus mechanisms are instrumental to detecting, eradicating and protecting against viral infections. Maintaining current malware definitions is absolutely necessary to ensure the highest degree of attainable defense against viral infection.

Anti-virus software should be installed on every desktop, laptop and server computer, especially in large organizations where strength in numbers is equally advantageous for viruses. In a server capacity, anti-virus software functions as a content filter between potentially hostile code and the intended recipient, perhaps in the form of an email attachment scanner.

Since anti-virus scanners are generally signature-based pattern matching engines with enhanced identification functionality, they are often limited to identifying only known sources of infection. There is some delay between the moment a new virus is born, to when it gets identified and reported to the proper authorities, and the issuance of virus signatures to identify the infector. Therefore it is crucial to maintain a timely and up-to-date signature database at all times.

Anti-virus scanning is best practiced in parallel at multiple layers of the network stack through enterprise-grade server solutions and end-user desktop applications. All new, off-site or unapproved software should be restricted from installation by any user until it is checked and cleared by administration and exposed to the network. Interconnection points, intermediary servers and endpoints are all susceptible to passing infected software and should be monitored closely.

Loading software only from trusted sources

Accepting signed and verified packages only from authorized content providers is one of the better ways to ensure reasonably safe software usage. Trusted vendors typically produce trustworthy software components, whereas executing code from an unverified third-party developer may lead to a potential security violation. This is not to say a trusted source cannot pass tainted goods, or that all unknown sources are based on bad intentions.

Making frequent backups

Frequent back-up and routine archival scheduling are the due diligence and good habits of a well-groomed administration staff that values advanced planning in the event of disaster. Ideally, incremental back-ups should be scheduled periodically, with full back-up jobs scheduled at less frequent intervals. A well-defined policy should clearly state the target material to be backed-up, the frequency at which back-ups occur and how they should be carried out.

Installing change detection software (integrity checker)

Checking and maintaining system-wide file or process integrity is a constant challenge for any computer security practitioner. Basic file integrity checking consists of an application that scours the entire disk drive seeking out file data for which to create signatures. These signatures are then matched against system files to detect any changes to the file data or metadata. Malware and malevolent end-users are constant sources of file and file system integrity compromise, and the best way to keep on top of any changes is through automated integrity-checking instrumentation, preferably with the signatures kept separately on a read-only medium. Some integrity-checking functionality is built into modern anti-virus engines, but even a standalone checker should be used in conjunction with other verification tools.

Implement a user awareness program

Users should be educated on how to identify potential sources of viral infection or malware activity, how to respond to these incidents, and the importance of following company policy regarding approved and validated software. End-users should also be aware of how their casual browsing and usage habits affect business operations and how their individual roles, responsibilities and responsiveness help to identify, isolate and investigate security incidents.

Risk, Response, and Recovery

Good security planning will provide preventative measures against all possible and conceivable risks, and then will define incident response in the event that the preventative measures fail.

Risk Management

Risk management is the business process of analyzing and mitigating risk. Risk management serves as the basis upon which a security policy is based. Once a security infrastructure is established, risk management serves as the testing, verification and improvement process to keep security solutions current and effective.

Risk management tools and methodologies

Risk management tools and methodologies include two primary focuses: quantitative and qualitative. Quantitative analysis assigns a hard dollar value to all assets. Qualitative evaluates opinions, beliefs and other forms of intangible assets. Both forms of analysis should be performed in order to produce a balanced perspective of the environment. A complete quantitative analysis cannot be performed without some qualitative expression, just as some qualitative/intangible items cannot be easily assigned a hard dollar value.

The principles of risk management

The principles of risk management include the identification of threats, vulnerabilities and risks; evaluating countermeasures and safeguards; providing senior management with sufficient information to make informed decisions about mitigation, assignment or acceptance of risk.

Risk Management Process

The risk management process is:

1. Inventory all assets and assign value to each asset.
2. Identify all possible risks to each asset to produce Risk-Asset pairs.
3. Define for each risk-asset pair the appropriate Exposure Factor percentage value.
4. Compute the Single Loss Expectancy for each Risk-Asset pair.
5. Calculate the Annualized Rate of Occurrence of each risk.
6. Calculate the Annual Loss Expectancy for each Risk-Asset pair.
7. Sort all Risk-Asset ALE values, then continue the process starting with the largest ALE value.
8. Inventory all possible countermeasures for each Risk.
9. Calculate the yearly cost to deploy each countermeasure.
10. Calculate a potential ARO and ALE for each countermeasure, as if it was applied/installed to the environment.
11. For each Risk-Asset pair, sort the post-counter measure ALEs.
12. Calculate the cost/benefit equation for each CM for each Risk-Asset pair: (ALE before – ALE after) – cost of the countermeasure.
13. Provide these results to senior management for their decisions on mitigation, assignment, and acceptance of each identified risk.
14. Use the senior management decisions to craft a security policy based on the selected countermeasures and safeguards.

Risk reduction/assignment/acceptance

The three valid responses to risk are: reduction, assignment and acceptance. Reduction or mitigation is the application of a countermeasure that eliminates or reduces a risk. Assignment is the purchasing of insurance or outsourcing in order to pass the risk on to others. Acceptance is the specific decision not to reduce or assign, but to live with the potential losses and consequences of a risk.

The risk which remains after the completion of the senior management decision process and all decisions are implemented is known as residual risk. Residual risk is the remaining risk after total risk is affected by countermeasures and safeguards. Residual risk is created by the gap in countermeasures.

Whatever residual risks remains after all senior management selected countermeasures are applied must be made clear and distinct in the minds of senior management. It is the responsibility of the security staff to ensure that senior management makes informed decisions and fully understands the consequences of all security decisions.

Incident Handling and Investigations

Any breach of security policy is an incident. Those incidents which are not automatically handled by the IT environment itself require human response to the issue. Some incidents can be fully handled in-house while others, specifically criminal incidents, require law enforcement involvement.

Security incidents

A security incident can be any form of security policy violation. That can include accidental as well as deliberate acts or actions of people, but can also include natural disasters. Security incidents may be caused by authorized users performing unauthorized actions, unauthorized users attempting to perform actions without approval, the presence of malicious code, terrorist attacks, receipt of individual or floods of spam, e-mail attachments or e-mail bombs, breaches of firewalls, social engineering attacks, traffic redirection attacks, sniffing and eavesdropping.

Incident response

Incident response is the pre-planned actions taken in the event of a security breach. Triggering incident response requires the ability to recognize attacks and escalate the notification of the attack along proper channels. It is important to keep control of the information regarding these incidents, as they can be used to repeat the security breach if made available to malicious entities.

In general, evidence collection should be left up to law enforcement. When evidence is collected, it should be protected from corruption or damage. A chain of custody document should be created once evidence is discovered, then that document should accompany the evidence and be updated throughout the life of that evidence through presentation in court.

Evidence should only be collected and handled by trained professionals. Any potential breach or compromise of the evidence should be proactively prevented. This includes accidental changes to magnetic storage media, proper temperature and humidity, prevention of dust, smoke, and debris from damaging the evidence, storage in paper bags, cardboard boxes, or static-proof electronic storage bags and prevention of theft and destruction.

Investigations

Investigations should be undertaken with care in order to minimize risk to the organization and ensure successful apprehension and prosecution of the suspect. Forensic investigation skills are required for a legal and successful investigation. This will include prevention of damage or loss of evidence due to the operation of the host computer. Thus, don't allow a graceful shutdown of the system, instead open the case and disconnect the power cable directly from the storage devices. All storage devices should be hashed using SHA-1 (or other approved hash algorithm) to use for integrity verification purposes, through the remaining life of the evidence.

Collection of evidence usually requires a search warrant issued by a judge. In order to obtain a search warrant, you must show a reasonable expectation that evidence of the crime exists, that evidence exists in a specific location and what type of evidence is expected to be present. Without a search warrant, evidence can be discarded by a judge if it cannot be shown to have had its integrity protected.

The act of the investigation can result in privacy violations (whether perceived or actual). Investigations can result in negative public opinion of the organization. Investigations may interrupt the normal production activities of the organization. Investigations may tip off the suspect and encourage them to perform retaliatory acts or flee capture or detection.

Interviewing is the act of talking with people in order to collect information regarding the "who," "what," "when," "where," "why" and how of a crime. This converts the person into a witness. Interrogation is the act of discovering that a witness may actually be the suspect. Then the act of interviewing is transformed into an attempt to illicit further evidence, self-incrimination or a confession.

Business Continuity Planning and Disaster Recovery

Business continuity planning (BCP) and disaster recovery planning (DRP) are designed to minimize the risk to an organization of downtime and outages due to incidents that cause reduction or destruction of business processes.

Business continuity planning process

The BCP planning process is comprised of four main steps or phases: scope and plan initiation, business impact assessment, business continuity plan development and plan approval and implementation. When performing BCP (or DRP) planning, you must incorporate any legal or regulatory requirements imposed on your organization and/or industry.

Scope and plan initiation will include criticality prioritization, resource requirements identification and downtime estimation (i.e. MTD or RTO).

Business impact assessment (a.k.a. business impact analysis or BIA) is the act of performing a risk assessment of business processes, rather than of assets. The overall process is the same. It should include both quantitative and qualitative assessments.

Plan development is the transformation of senior management's decisions on the results of the BIA into a procedural document. The BCP should include a backup and restoration strategy that includes offsite storage of backup media. In general, the recovery strategy of a BCP focuses on the most mission critical processes first. Proper BCP may require service level agreements with partners, hardware vendors or service providers. Plan approval and implementation includes the roll-out of the finished and senior management approved plan, user awareness, training and drilling, as well as plan maintenance. As plan updates are distributed, all old copies of the plan should be removed and destroyed.

Disaster recovery planning process

The DRP process is basically the same as that of BCP, however at least one additional step is needed: data processing continuity planning.

Data processing continuity planning is the process of selecting or developing a response strategy in the event of primary systems failure. Common options are: hot site, warm site, cold site, mutual aid agreement (a.k.a. reciprocal agreement), service bureaus, multiple centers, dual sites and mobile/portable sites. When selecting an alternate processing site, it is important that site be far enough away from the primary site so as not to be affected by the same disaster, but close enough that workers can travel there in a reasonable amount of time. If the alternate site is located far away, room and board arrangements for workers will need to be arranged.

Response Teams

When BCP or DRP is triggered, the team of workers implementing the plan is called the recovery team. Their job is to maintain or restore mission critical processes. In most cases, the recovery team's tasks must be successfully completed in a short amount of time (e.g. MTD or RTO).

Once the business is stable, in the event of a DRP event, a salvage team is needed to rebuild the primary site and return the organization back to normal operations at the re-created primary site. Since returning to the rebuilt site can cause a second disaster, the emergency is not over until the organization has all mission critical functions performing reliably at the new primary site. The salvage team often has a longer time frame within which to perform their tasks. The least mission critical processes are transferred to the rebuilt primary site in order to establish reliability and resilience as more important tasks are transferred.

Plan Testing

Both BCP and DRP should be tested. Testing identified plan deficiencies trains personnel, verifies the capability of alternate processing solutions and informs the organization whether or not the plans are mature enough to perform reliably in a real emergency.

There are five plan testing options. Two are paper based tests: checklist and structured walk-through (i.e. group discussion). Three are real-world tests: simulation, parallel and full interruption.

Practice Questions

Chapter 1 Access Control

1. Designing a proper access control system requires that you address three primary concerns, the least important being which of the following?
Select the best answer.
 - A. Threat level.
 - B. Risk factor
 - C. Loss expectancy.
 - D. Vulnerability status.

2. There are three primary classifications for access control models. Identify one of the following entries that best describes one of these models.
Select the best answer.
 - A. Resource-based
 - B. Mandatory
 - C. Reason-based
 - D. Modular

3. Which of the following mechanisms is not likely used as a form of biometric authentication?
Select the best answer.
 - A. Voice pattern identification.
 - B. Retinal scan.
 - C. Fingerprint analysis.
 - D. Hair follicle test.

4. Implementing the authentication mechanisms by which access is controlled requires an accurate understanding of a few basic principles. Which of the following statements about authentication factors is not accurate?
Select the best answer.
 - A. Authentication is the process of proving an individual's identity.
 - B. Any good authentication factor by itself is stronger than several weak factors combined.
 - C. Something you are and something you have are factors included in two-factor and multi-factor systems.
 - D. Functions and activities of the human body can be used as authentication factors.

5. Which of the following mechanisms is not likely used as a form of biometric authentication?
Select the best answer.
- A. Voice pattern identification.
 - B. Retinal scan.
 - C. Fingerprint analysis.
 - D. Hair follicle test.
6. The act of convincing a third party to participate in a criminal act on behalf of another individual is better known as what?
Select the best answer.
- A. Collusion.
 - B. Confidentiality.
 - C. Non-repudiation.
 - D. Separation of duties.
7. Which of the following security attributes is not applicable to Mandatory Access Control-based configurations?
Select the best answer.
- A. Multi-level security architecture.
 - B. Discretionary permissions.
 - C. Layer-based security architecture.
 - D. Universal coverage.
8. Which of the following answer choices provides a high-level overview of how security is perceived throughout an entire organization?
Select the best answer.
- A. Standards.
 - B. Policies.
 - C. Guidelines.
 - D. Procedures.

Chapter 2 Administration

1. Holding a person responsible for the activities performed using his or her assigned credentials is best described by what terminology?
Select the best answer.
- A. Confidentiality.
 - B. Accountability.
 - C. Integrity.
 - D. Non-repudiation.

2. If identification is the process of claiming a given identity, what is the purpose of authentication? Select the best answer.
- A. To prove that identity as belonging to the individual claiming it for accountability purposes.
 - B. To hold an individual responsible for the actions performed under the credentials of a given identity.
 - C. To protect against an individual's ability to deny responsibility for out-of-policy or criminally negligent activity in his or her account.
 - D. To enforce a level of accessibility to valid resources for the users authorized to utilize them.
3. Layering is a logical ordering of similar security domains in a consolidated hierarchy from low to high. Why is layering used? Select the best answer.
- A. To classify subjects separately from objects for identification purposes.
 - B. Layering enables administrators to enforce responsibility for subjects as they interact with other subjects and objects.
 - C. Layering provides classification labels for objects and subjects so that high-priority information is hidden from lower-level entities.
 - D. Layering lays the basis for which intranet policies and user agreements are derived.
4. Levels of secrecy, isolation, and seclusion to assume protection for individuals and their possessions is called what? Select the best answer.
- A. Privacy.
 - B. Separation of Duties.
 - C. Confidentiality.
 - D. Integrity.
5. Disclosure of sensitive information is best serviced by what core security administration principle? Select the best answer.
- A. Integrity.
 - B. Accountability.
 - C. Availability.
 - D. Confidentiality.
6. Which of the following definitions best describes the act of observing the passage of information between systems without examination of its content? Select the best answer.
- A. Replay attack.
 - B. Data hiding.
 - C. Traffic analysis.
 - D. Disclosure.

7. What typically is considered the weakest link of any security administration paradigm?
Select the best answer.
- A. Resources.
 - B. Policies.
 - C. Privacy.
 - D. People.
8. The regulation of changes and modifications to system properties, parameters, and preferences is better known by what security terminology?
Select the best answer.
- A. Configuration management.
 - B. Data classification.
 - C. Authentication scheme.
 - D. Policy writing.

Chapter 3 Audit and Monitoring

1. What is the primary goal of any comprehensive top-down security audit and monitoring process?
Select the best answer.
- A. To classify objects and subjects of an organization with security labels and corresponding privileges.
 - B. To establish a baseline of security by which all policies, procedures, guidelines, and standards are derived.
 - C. To assess potential risk factor as it applies to possible monetary losses due to exploitation or exposure.
 - D. To verify compliance with security policy and detect violations of that policy.
2. Different control function types protect valuable assets in a number of ways. Which of the following methods lends guidance to achieving compliance with other controls and restrictoins?
Select the best answer.
- A. Directive.
 - B. Preventative.
 - C. Detective.
 - D. Corrective.

3. What is usually the first standard goal to be achieved during a formal internal security audit?
Select the best answer.
- A. Problem identification.
 - B. Problem resolution.
 - C. Problem marginalization.
 - D. Problem avoidance.

Chapter 4 Risk, Response and Recovery

1. Calculating total risk is simply a matter of knowing the right formula. Which of the following answers best describes this formula?
Select the best answer.
- A. $\text{Threat} \times \text{Vulnerability} / \text{Annual Loss Expectancy} = \text{Total Risk}$
 - B. $\text{Threat} \times \text{Vulnerability} \times \text{Asset Value} = \text{Total Risk}$
 - C. $\text{Threat} / \text{Vulnerability} \times \text{Annual Loss Expectancy}$
 - D. $\text{Threat} / \text{Vulnerability} \times \text{Asset Value} = \text{Total Risk}$
2. Risk is defined as the potential for damage to occur as applied to an organization, its people, and resources. Which of the following statements most likely corresponds to risk management?
Select the best answer.
- A. The process of identifying, assessing, and reducing risk to an acceptable level.
 - B. The process of perceiving, assigning, and eliminating risk factors to an optimal level.
 - C. A method of identifying risk and assessing potential damage to position security solutions and safeguard an infrastructure.
 - D. A method of calculating the monetary losses sustained from potential risk factors.
3. Risk defines the potential of a threat overtaking a vulnerability and leading to exploitation or exposure. What is the simple formula for calculating risk?
Select the best answer.
- A. $\text{Risk} = \text{Threat} \times \text{Vulnerability}$.
 - B. $\text{Risk} = \text{Threat} \times \text{Exposure}$.
 - C. $\text{Risk} = \text{Threat} / \text{Vulnerability}$.
 - D. $\text{Risk} = \text{Threat} / \text{Exposure}$.

Chapter 5 Cryptography

1. Cryptographic systems are designed to operate on a few key concepts. Among the following choices, which statement is not one of these concepts?
Select the best two answers.
 - A. Access is restricted only to authorized parties.
 - B. Validation of origin and identify for any message us necessary.
 - C. Assurances can be made that the message arrives in original form, completely free of modification or tampering by any external source.
 - D. The sender of a message should be able to deny having sent a message especially if the contents of that message may be damaging to the sender's reputation.

Chapter 6 Data Communications

1. The International Standards Organization developed a universally recognized layered protocol reference model by which TCP/IP is best illustrated. Which answer appears as the third layer of this model?
Select the best answer.
 - A. Physical.
 - B. Presentation.
 - C. Session.
 - D. Network.

Chapter 7 Malicious Code and Malware

1. Malicious code is a constant danger to any secured computer infrastructure. Which of the following malicious code agents is self-replicating across the network?
Select the best answer.
 - A. A virus.
 - B. A worm.
 - C. A Trojan horse.
 - D. A logic bomb.

Answers and Explanations

Chapter 1

1. Answer: C

Explanation A. The threat level is a measurable quantity of threat posed to a particular organization and its assets and must be understood to properly position access controls.

Explanation B. Risk is the potential for damage to occur and it factors directly into controlling access to users and resources.

Explanation C. Loss expectancy relates to the calculated costs associated with risk as it applies to computer systems and infrastructures.

Explanation D. Vulnerability describes a weakness that can lead to exploitation and system compromise, which clearly should be a concern for any access control system.

2. Answer: B

Explanation A. Access controls protect resources, but as a classification this label is inaccurate and incorrect.

Explanation B. Mandatory Access Controls (MAC) are a categorical form of access control mechanisms.

Explanation C. Access control mechanisms are driven by reason (or policy) but not defined specifically as such.

Explanation D. Modularity may be an underlying aspect to a given access control mechanism, but no such implementation is classified as such.

3. Answer: D

Explanation A. Voice pattern fingerprinting technology is a valid method of authenticating users by accurately identifying an individual.

Explanation B. Scanning the retina of an individual remains one of the most reliable methods of authenticating users working in high security clearance areas.

Explanation C. Fingerprint analysis is well-understood as a means of uniquely identifying an individual and a method of authentication used for access control.

Explanation D. Though an accurate means of identifying an individual or characteristics about an individual, this method is least likely to appear anywhere as a means to authenticate a person.

4. Answer: B

Explanation A. This is true and describes an aspect of access control.

Explanation B. This statement is false. Any single factor is considered weak in comparison to multiple authentication factors of any kind.

Explanation C. When combined with the third generally recognized factor, something you know, these ele-

ments make up the parameters by which any good user authentication system is designed.

Explanation D. Some functions can be utilized in a security context to authenticate users by seeking to distinguish unique behavioral characteristics, such as keystroke events.

5. Answer: D

Explanation A. Voice pattern fingerprinting technology is a valid method of authenticating users by accurately identifying an individual.

Explanation B. Scanning the retina of an individual remains one of the most reliable methods of authenticating users working in high security clearance areas.

Explanation C. Fingerprint analysis is well-understood as a means of uniquely identifying an individual and a method of authentication used for access control.

Explanation D. Though an accurate means of identifying an individual or characteristics about an individual, this method is least likely to appear anywhere as a means to authenticate a person.

6. Answer: A

Explanation A. This answer is correct.

Explanation B. Confidentiality describes a level of secrecy or privacy but does not imply incorrect behavior or activity.

Explanation C. Non-repudiation is the ability to deny ownership for a given message or responsibility for a given act.

Explanation D. This answer is incorrect because it employs the principle of least privilege in regard to legitimate system usage.

7. Answer: B

Explanation A. This answer is correct because MAC-based control schemes are based on a multi-level security architecture.

Explanation B. This answer is incorrect because discretionary permissions on behalf of the user belongs to Discretionary Access Control schemes.

Explanation C. This answer is correct because MAC is a layered security framework.

Explanation D. This answer is correct because MAC-based controls cover the entire universe of hardware, software, and users under said control.

8. Answer: B

Explanation A. This answer is incorrect because standards specify how organizational resources are used, not how their correct or incorrect usage is perceived.

Explanation B. This answer is correct.

Explanation C. This answer is incorrect because guidelines merely describe recommended actions and activities for users where no specific standards apply.

Explanation D. This answer is incorrect because procedures describe the procedural how-to side of security administration.

Chapter 2

1. Answer: B

Explanation A. Confidentiality is a protective measure against disclosure of sensitive information to unauthorized parties.

Explanation B. Accountability is absolutely essential to any security paradigm since users should be held responsible for all activities performed or content created, passed, and modified.

Explanation C. Integrity is the assurance that stored information remains unmodified when it is later retrieved.

Explanation D. Non-repudiation is a protective measure against the ability for an individual to deny ownership or responsibility for a given piece of information or deliberate action.

2. Answer: A

Explanation A. This answer is correct.

Explanation B. This answer is incorrect. It describes accountability, which is comprised of identification and authentication.

Explanation C. This answer is incorrect. It describes non-repudiation, which is based on an individual being both identified and authenticated.

Explanation D. This answer is incorrect because it describes availability.

3. Answer: C

Explanation A. This answer is incorrect because it only partly describes how layering is used.

Explanation B. This answer is incorrect because it more accurately describes accountability.

Explanation C. This answer is correct.

Explanation D. This answer is incorrect because it does not accurately describe the purpose of layering.

4. Answers: A

Explanation A. This answer is correct.

Explanation B. Incorrect. Separation of duties (also known as the principle of least privilege) is the logical division of job responsibilities to prevent fraudulent activity.

Explanation C. This answer is incorrect because confidentiality is the protection of private information against disclosure to unauthorized parties.

Explanation D. This answer is incorrect because integrity is the assurance that information is correct and unmodified from its original form.

5. Answer: D

Explanation A. Incorrect. Integrity means that a given piece of information is complete, accurate, and unchanged from its original form (except by the authorized parties).

Explanation B. This answer is incorrect because accountability is used to establish responsibility for a given user account.

Explanation C. This answer is incorrect because availability is concerned with assuring that resources are made available to the appropriate users.

Explanation D. Confidentiality assures protection against disclosure of information and is the basis for various forms of privacy.

6. Answer: C

Explanation A. This answer is incorrect because the observation is non-intrusive and does not examine contents, let alone re-use messages at a later time.

Explanation B. This answer is incorrect because data hiding is related to privilege separation with respect to objects and subjects.

Explanation C. This is the correct answer.

Explanation D. This answer is incorrect because no messages are ever viewed for their contents but rather their correspondence between systems.

7. Answer: D

Explanation A. This answer is incorrect because resources can be among the better secured and audited properties of any security paradigm.

Explanation B. This answer is incorrect because the quality of a policy cannot safeguard against the weakest link in every security chain.

Explanation C. This answer is incorrect because privacy is not considered a weakness of any security paradigm (unless it is absent of any privacy).

Explanation D. This answer is correct.

8. Answer: A

Explanation A. This answer is correct.

Explanation B. This answer is incorrect because classifying data only serves to define the policies that govern how such elements are used.

Explanation C. This answer is incorrect because an authentication scheme only controls certain basic access to and from systems but provides no extensive coverage to how those systems are used.

Explanation D. This answer is incorrect because policy writing does not regulate access or modification to system properties, parameters, or preferences.

Chapter 3

1. Answer: D

Explanation A. This answer is incorrect because security classification is something that should occur before any formal audit and monitoring process can be established.

Explanation B. This answer is incorrect because the audit and monitoring process should evaluate these aspects, not necessarily form them.

Explanation C. This answer is incorrect because it belongs in the category of risk and risk management.

Explanation D. This answer is correct.

2. Answer: A

Explanation A. This answer is correct.

Explanation B. This answer is incorrect because preventative measures are designed to prevent security policy violations.

Explanation C. This answer is incorrect because detective controls identify security violations.

Explanation D. This answer is incorrect because corrective measures seek to restore order to an environment following a security violation incident.

3. Answer: A

Explanation A. This answer is correct.

Explanation B. This answer is incorrect because problem resolution happens subsequent to the first goal to be achieved.

Explanation C. This answer is incorrect because no security problem should be marginalized for any reason.

Explanation D. This answer is incorrect primarily because no security problem should ever be avoided especially where discovered by a security audit or monitoring process.

Chapter 4

1. Answer: B

Explanation A. This answer is incorrect as the formula does not make sense in the context of risk management.

Explanation B. This answer is correct.

Explanation C. This answer is incorrect and does not represent a valid risk-related formula.

Explanation D. This answer is incorrect and is only a distracter.

2. Answer: A

Explanation A. This answer is correct.

Explanation B. This answer is incorrect mainly because it includes the term elimination-risk can never be eliminated.

Explanation C. This answer is incorrect because it more accurately describes risk analysis.

Explanation D. This answer is incorrect because it refers to calculating total risk, which is only a part of risk management.

3. Answer: A

Explanation A. This answer is correct.

Explanation B. This answer is incorrect because threat multiplied by exposure makes no sense in a security context.

Explanation C. This answer is incorrect because threat cannot be divided by vulnerability.

Explanation D. This answer is incorrect because threat cannot be divided by exposure.

Chapter 5

1. Answers: C, D

Explanation A. Restricted access is entirely necessary to adequately secure confidential information from exposure to the wrong sources.

Explanation B. A cryptosystem requires the ability to accurately and unmistakably identify the true source and identify for all corresponding messages.

Explanation C. Integrity-verifying the correctness of a message upon arrival-is essential to any worthy cryptosystem.

Explanation D. This statement is false. Part of the strength of any cryptosystem lies in its ability to undeniably identify the source of origin for any given message.

Chapter 6

1. Answer: D

Explanation A. This answer is incorrect because the physical layer occurs below the third reference layer.

Explanation B. This answer is incorrect because the presentation layer occurs above the third layer.

Explanation C. This answer is incorrect because the session layer occurs above the third reference layer.

Explanation D. This answer is correct.

Chapter 7

1. Answer: B

Explanation A. This answer is correct because viruses by design are transmittable only to local resources, except where network storage drives are mapped locally.

Explanation B. This answer is correct.

Explanation C. This answer is incorrect because a Trojan horse usually replicates by itself and requires the assistance of a delivery mechanism.

Explanation D. This answer is incorrect because a logic bomb does not necessarily replicate nor transmit itself over a network.