



**CBK#1 ACCESS CONTROL SYSTEMS
& METHODOLOGY**

**CBK#2 TELECOMMUNICATIONS &
NETWORK SECURITY**

**CBK#3 SECURITY MANAGEMENT
PRACTICES**

**CBK#4 APPLICATIONS & SYSTEMS
DEVELOPMENT SECURITY**

CBK#5 CRYPTOGRAPHY

**CBK#6 SECURITY ARCHITECTURE &
MODELS**

CBK#7 OPERATIONS SECURITY

**CBK#8 BUSINESS CONTINUITY
PLANNING & DISASTER RECOVERY**

**CBK#9 LAW, INVESTIGATIONS &
ETHICS**

CBK#10 PHYSICAL SECURITY

CISSP Summary 2002

By John Wallhoff (CISA, CISSP)

Written by: J.Wallhoff January - April 2002
Updated by: J.Wallhoff September 2005

CISSP Summary 2002

I wrote this summary as a part of the preparation for my CISSP exam. It is based on books and different sources found on the Internet. You may use it as a part of your preparation, but it doesn't replace the CISSP seminars or books available.

The summary covers all the ten Common Body of Knowledge Domains (CBK) that are required for the CISSP Exam. I have also added a page for related links and references that might be useful. This page is far from complete and there is a lot more to be found.

My recommendation to anyone planning to sit for the exam, is to make a study plan of your own. Some of you might have been involved in all of the domains already, but I guess most of you will find a few domains easier and other domains a bit harder. I studied for 2 1/2 month on my spare time (late in the evening when my kids went to bed), all the time uncertain if I read too much or too little. I did pass the exam but still I don't know if I read too much or too little.

During my preparation, I have seen questions about CISSP versus CISA. The focus of those two certifications is different. While CISSP is focused on building and maintain security, CISA is more focused on auditing and assessing risks and controls. Your choice of certification should be based on what you really want to work with. If you want to be a security professional, CISSP is the choice. If you want to be an IT/IS auditor instead, then you should take CISA. As I've been an IT/IS auditor and now is an IS consultant, I ended up with both. So far I have used the knowledge supported by both CISA and CISSP.

Last but not least for your preparation. Once upon a time, a teacher at the university told my class "four in - five out". That wasn't about how many hours you should use for your exam. That was how many hours you should allow yourself to sleep, to be able to pass the exam. If you slept four hours at the most each night, you would probably make it. If you slept five hours, you were likely to fail. For your comfort I slept more than five hours each night and I passed. So for all of you preparing for the exam, quality time is much better than quantity.

Good luck to all of you still convinced to take the exam.

John Wallhoff

About the updated version.
Statement about warm site is changed

Index

Index.....	3
CBK#1 Access Control Systems & Methodology	4
CBK#2 Telecommunications & Network Security.....	12
CBK#3 Security Management Practices	22
CBK#4 Applications & Systems Development Security	27
CBK#5 Cryptography	36
CBK#6 Security Architecture & Models	44
CBK#7 Operations Security	53
CBK#8 Business Continuity Planning & Disaster Recovery Planning	59
CBK#9 Law, Investigations & Ethics	63
CBK#10 Physical Security	67
Related links	72
References	73

CBK#1 Access Control Systems & Methodology

Security principles

Confidentiality:

The assurance that information is not disclosed to unauthorized individuals, programs or processes.

Integrity:

Information must be accurate, complete and protected from unauthorized modification.

Availability:

Information, systems and resources need to be available to users in a timely manner so productivity will not be affected.

Identification

Describes a method of ensuring that a subject (user, program or process) is the entity it claims to be. Identification can be verified through the use of a credential.

Biometrics:

Verifies an individual's identity by a unique personal attribute, which is one of the most effective and accurate methods of verifying identification.

Three main performance measures -

- FRR / False Rejection Rate or Type I Error - The percentage of valid subjects that are falsely rejected.
- FAR / False Acceptance Rate or Type II Error - The percentage of invalid subjects that are falsely accepted.
- CER / Crossover Error Rate - The percent in which the False Rejection Rate equals the False Acceptance Rate.

Other factors that must be considered -

- Enrolment time - The time it takes to initially "register" with a system by providing samples of the biometric characteristic to be evaluated.
- Throughput rate - The rate at which individuals can be processed and identified or authenticated by a system.
- Acceptability - Considerations of privacy, invasiveness and psychological and physical comfort when using the system.

Types of biometric systems -

Fingerprints: Are made up of ridge endings and bifurcations exhibited by the friction ridges and other detailed characteristics that are called minutiae.

Palm Scan: The palm has creases, ridges and grooves throughout it that are unique to a specific person.

Hand Geometry: The shape of a person's hand (the length and width of the hand and fingers) measures hand geometry.

Retina Scan: Scans the blood-vessel pattern of the retina on the backside of the eyeball.

Iris Scan: Scan the colored portion of the eye that surrounds the pupil.

Signature Dynamics: Electrical signals of speed and time that can be captured when a person writes a signature.

Keyboard Dynamics: Captures the electrical signals when a person types a certain phrase.

Voice Print: Distinguishing differences in people's speech sounds and patterns.

Facial Scan: Takes attributes and characteristics like bone structures, nose ridges, eye widths, forehead sizes and chin shapes into account.

Hand Topology: Looks at the size and width of an individual's hand and fingers.

Authentication

The subject is required to provide a second piece to the credential set.

Passwords:

Is a protected string of characters that is used to authenticate an individual.

Clipping level - An allowed number of failed logon attempts to happen before a user is locked out.

Password checkers - Test of user-chosen passwords.

Password Generators - Generators that produce users' passwords.

Password Aging - Expiration dates for passwords.

Limit Login Attempts - Threshold set to allow only a certain number of unsuccessful login attempts.

Cognitive password:

Fact- or opinionbased information used to verify an individual's identity.

One-time passwords / dynamic password:

After the password is used, it is no longer valid.

Token Device:

Is a password generator that uses a challenge response scheme.

Synchronous token device - Synchronizes with the authentication service by using time or an event as the core piece of the authentication process.

Time based synchronous token device - The device and the authentication service must hold the exact same time within their internal clocks.

Event-synchronization - The user may need to initiate the logon sequence on the computer and push a button on the token device.

Asynchronous token device - Uses challenge-response scheme to communicate with the authenticate with the authentication service.

Cryptographic Keys:

Presenting a private key or a digital signature.

Passphrase:

Is a sequence of characters that is longer than a password. The user enters this phrase into an application and the application transforms the value into a virtual password.

Memory Card:

A card that holds information, but does not process information.

Smart Card:

A card that has the capability of processing information because it has a microprocessor and integrated circuits incorporated into the card itself.

A smart card also provides a two-factor authentication method because the user has to enter a user ID and PIN to unlock the smart token.

Authorization

Granting access to a subject to an object after the object has been properly identified and authenticated.

Need-to-know:

Users will only have the necessary rights and permissions they need to fulfil the obligations of their jobs within the company.

Single Sign-on

Capabilities that would allow a user to enter credentials one time and be able to access all resources in primary and secondary network domains.

Scripting:

Batch files and scripts that contain each user's ID, password and logon commands necessary for each platform.

Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully.

Kerberos:

Uses symmetric key cryptography and provide end-to-end security

Main components -

- KDC / Key Distribution Center:

Holds all users' and services' cryptographic keys. It provides authentication services, as well as key distribution functionality. The KDC provides security services to entities referred to as principals, that can be users, applications or services.

A ticket is generated by the KDC and given to a principal when that principal needs to authenticate to another principal.

A KDC provides security services for a set of components and principals. This is called realm in Kerberos.

- AS / Authentication Service:

Is the part of the KDC that authenticates a principal

- TGS / Ticket Granting:

Is the part of KDC that makes the tickets and hands them out to the principals.

Weaknesses -

The KDC is a single point of failure

The AS must be able to handle a huge amount of requests.

Secret keys are temporarily stored on users' workstations.

Session keys are decrypted and reside on the users' workstations.

Is vulnerable to password guessing.

Network traffic is not protected

When a user changes his password, it changes the secret key and the KDS needs to be updated.

SESAME:

Uses public key cryptography for the distribution of secret keys.

Uses a ticket for authorization which is called a Privilege Attribute Certificate.

Is vulnerable to password guessing.

Thin Clients:

Dump terminals authenticating to a server.

Access Control Models

Is a framework that dictates how subjects access objects.

DAC / Discretionary Access Control:

Enables the owner of the resource to specify what subjects can access specific resources.

Access is restricted based on the authorization granted to the users.

The most common implementation of DAC is through ACL's

MAC / Mandatory Access Control:

Users are given a security clearance and data is classified.

The classification is stored in the security labels of the resources.

When the system makes a decision about fulfilling a request to access an object, it is based on the clearance of the subject and the classification of the object.

The model is used in environments where information classification and confidentiality is of utmost importance.

Sensitivity labels:

When MAC is used every subject and object must have a sensitivity label. It contains classification and different categories. The classification indicates the sensitivity level and the categories indicate which objects take on the classification.

RBAC / Role-based access control:

Also called nondiscretionary access control.

Uses a centrally administrated set of controls to determine how subjects and objects interact.

Allows access to resources based on the role the user holds within the company.

RBAC models can use -

- Role-based access: Determined by the role the user has within the company.
- Task-based access: Determined by the task assigned to this user.
- Lattice-based access: Determined by the sensitivity level assigned to the role.

Access Control Techniques and Technologies

Techniques and technologies available to support different access control models.

Role-Based Access Control:

Based on the tasks and responsibilities that individuals need to accomplish to fulfil the obligations of their positions in the company.

RBAC can be used with -

- DAC, administrators can develop roles and owners can decide if these roles can have access to their resources.
- MAC, roles can be developed and sensitivity labels assigned to those roles indicating its security level.

Rule-Based Access Control:

Based on specific rules that indicate what can and cannot happen to an object.

Is a type of MAC because the administrator sets the rules and the users cannot modify these controls.

Restricted Interfaces:

Restrict users' access abilities by not allowing them to request certain functions, information or have access to specific system resources.

Three types of restricted interfaces -

- Menus and shells: Users are only given the options of the commands they can execute.
- Database views: Are mechanisms used for restricting user access to data that is contained in databases.
- Physically constrained interfaces: Can be implemented by only providing certain keys on a keypad or touch buttons on a screen.

Access Control Matrix:

Is a table of subjects and objects indicating what actions individual subjects can take upon individual objects.

Is usually an attribute of DAC models and the access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs).

Capability Tables:

Specifies the access rights a certain subject possesses pertaining to specific objects.

The subject is bound to the capability table.

Is used in Kerberos.

Access Control Lists:

They are lists of subjects that are authorized to access a specific object and they define what level of authorization is granted.

Authorization can be specified to an individual, role or group.

Content-Dependent Access Control:

Access to objects is determined by the content within the object.

Access Control Administration

Centralized:

One entity (department or individual) is responsible for granting all users access to resources.

Provides a consistent and uniform method of controlling users' access rights.

Examples of centralised access control technologies:

- Radius / Remote Authentication Dial-in User Service:

Is an authentication protocol that authenticates and authorizes users usually dial-up users.

- TACACS / Terminal Access Controller Access Control System:

Is a client/server protocol that provides the same type of functionality as Radius.

Three generations -

- * TACACS - Combines authentication and authorization.

- * XTACACS - Separates authentication, authorization and accounting processes.

* TACACS+ - Separates authentication, authorization and accounting processes, with extended two-factor user authentication.

Decentralized and Distributed Access Administration:

Gives control of access to the people closer to the resources.

Does not provide uniformity and fairness across the organizations.

Examples of decentralized access control administration techniques.

Security Domain -

Can be described as a realm of trust.

All subjects and objects share common security policies, procedures and rules and they are managed by the same management system.

Each security domain is different because different policies and management govern it.

Can be implemented in hierarchical structures and relationships.

Are used within operating systems and applications to ensure that rogue activities do not accidentally damage important system files or processes.

Protection of security level is done through segmenting memory spaces and addresses.

A security domain can also be described as the resources available to a user.

Hybrid:

Is a combination of the centralized and decentralized access control administration methods.

Access Control Methods

Administrative Controls:

Policy and Procedures -

Is a high level plan stating management's intent pertaining to how security should be practiced within an organization, what actions are acceptable and what level of risk the company is willing to accept. Senior management will decide if DAC, MAC or RBAC access methodology should be used and if it should be administered via centralization or decentralization.

Personal Controls -

Indicate how employees are expected to interact with security mechanisms and noncompliance issues pertaining to these expectations.

- Separation of duties: Not one individual can carry out a critical task alone that could prove to be detrimental to the company.

- Collision: More than one person would need to commit fraud and this effort would need to happen in a concerted effort.

- Rotation of duties: People need to know how to fulfil the obligations of more than one position.

Supervisory Structure -

Each employee has a superior to report to and that superior in return is responsible for that employee's actions.

Security Awareness Training -

People are usually the weakest link and cause the most security breaches and compromises.

Testing -

All security controls and mechanisms need to be tested on a periodic basis to ensure they properly support the security policy, goals and objectives set for them.

Physical Controls:

Network Segregation -

Can be carried out through physical and logical means.

Perimeter Security -

Mechanisms that provide physical access control by providing protection for individuals, facilities and the components within facilities.

Computer Control -

Physical controls installed and configured.

Work Area Separation -

Controls that are used to support access control and the overall security policy of the company.

Data Backups -

Ensure access to information in case of an emergency or a disruption of the network or a system.

Cabling -

All cables need to be routed throughout the facility in a manner that is not in people's way or that could be exposed to any danger of being cut, burnt, crimped or eavesdropped upon.

Logical Controls:

System Access -

A technical control that can enforce access control objectives.

Network Architecture -

Can be constructed and enforced through several logical controls to provide segregation and protection of an environment. Can be segregated physically and logically.

Network Access -

Access to different network segments should be granular in nature. Routers and switches can be used to ensure that only certain types of traffic get through to each segment.

Encryption and protocols -

Works as technical controls to protect information as it passes throughout a network and resides on computers.

Control Zone -

Is a specific area that surrounds and protects network devices that emit electrical signals.

Auditing -

Technical controls that track activity within a network, on a network device or on a specific computer.

Access Control Types

(P - Physical / A - Administrative / T - Technical)

Preventative: Controls used to deter and avoid undesirable events from taking place.

P - Fences, Locks, Badge System, Security guard, Biometric system, Mantrap door, Lighting, CCTV, Alarms

A - Security policy, Monitoring and supervising, Separation of duties, Job rotation, Information Classification, Personnel procedures, Testing, Security awareness training.

T - ACLs, Routers, Encryption, IDS, Antivirus software, Firewalls, Smart cards, Dial-up call-back systems.

Detective: Controls used to identify undesirable events that have occurred.

P - Security guard, Biometric system, Motion detectors, CCTV, Alarms, Backups.

A - Monitoring and supervising, Job rotation, Personnel procedures, Investigations, Security awareness training.

T - Audit logs, IDS, Antivirus software, Firewalls.

Corrective: Controls used to correct undesirable events that have occurred.

P - Fences, Locks, Badge System, Security guard, Biometric system, Mantrap door, Lighting, CCTV, Alarms

A - Security policy.

T - IDS, Antivirus software.

Deterrent: Controls used to discourage security violations.

P - Backups

A - Monitoring and supervising, Separation of duties, Personnel procedures.

T - Encryption, IDS, Firewalls.

Recovery: Controls used to restore resources and capabilities.

P - Fences, Locks, Security guard, Mantrap door, Lighting, Alarms, Backups

A -

T - Antivirus software.

Compensation: Controls used to provide alternatives to other controls.

P -

A - Monitoring and supervising, Personnel procedures.

T -

Review of audit information:

Audit reduction - Reduces the amount of information within an audit log.

Variance-detection tool - Monitor computer and resource usage trends and detect variations.

Attack signature-detection tool - The application will have a database of information that has been known to indicate specific attacks.

Keystroke Monitoring:

Review and record keystrokes entered by a user during an active session.

Access Control Monitoring

IDS / Intrusion detection:

Network-based - Monitors a network or a segment of the network.

Host-based - Monitors a particular system.

Knowledge-based / signature-based - Models of how the attacks are carried out are developed.

Behaviour-based / Statistical - Observes and detects deviation from expected behaviour of users and systems.

TIM / Time-based induction machine - perform real-time anomaly detection.

Honeypot - A "fake" system that is not locked down and has open ports and services enabled within the network.

Network sniffers - Is a type of wiretap that plugs into a network for the purpose of eavesdropping on network traffic.

Threats to Access Control

Dictionary Attack:

Programs that enable an attacker to identify user credentials. The program is fed lists of commonly used words or combinations of characters, and the program applies these values to a logon prompt.

Brute Force Attack:

An attack that continually tries different inputs to achieve a predefined goal. Are also used in wardialing efforts.

Spoofing at Login:

A program that presents a fake login screen, to obtain user credentials.

CBK#2 Telecommunications & Network Security

Open System Interconnect Model

Protocol - Standard set of rules that determine how systems will communicate across networks.

OSI Model	TCP/IP
Application	Application
Presentation	
Session	
Transport	Host-to-host
Network	Internet
Data Link	Network Access
Physical	

Each layer adds its own information to the data packet.

7. Application layer:

Processes and properly formats the data and passes it down to the next layer.

Protocols used - SMTP, HTTP, LPD, FTP, WWW, Telnet, TFTP.

6. Presentation layer:

Provides a common means of representing data in a structure that can be properly processed by the end system.

Formats Graphic into TIFF, GIF or JPEG.

Handles data compression and encryption.

5. Session layer:

Establishing a connection between the two computers, maintaining it during the transferring of data and controlling the release of this connection.

Protocols used - SSL, NFS, SQL, RPC

4. Transport layer:

Provides end-to-end data transport services and establishes the logical connection between two communicating computers.

Protocols used - TCP, UDP, SPX

Information is passed down from different entities at higher layers to the transport layer, which must assemble the information into a stream.

3. Network layer:

Insert information into the packet's header so that it can be properly routed.

Protocols used - IP, ICMP, RIP, OSPF, BGP, IGMP.

Protocols that work at this layer do not ensure the delivery of the packets.

2. Data Link layer:

The operating system format the data frame to properly transmit over networks (Token Ring, Ethernet, ATM or FDDI).

Protocols used - SLIP, PPP, RARP, L2F, L2TP, FDDI, ISDN

Each network technology has defined electronic signalling and bit patterns.

1. Physical layer:

Converts bits into voltage for transmission.

Standard interfaces - HSSI, X.21, EIA/TIA-232, EIA/TIA-449

The session layer enables communication between two computers to happen in three different modes:

- Simplex: Communication takes place in one direction.

- Half-duplex: Communication takes place in both directions, but only one system can send information at a time.
- Full-duplex: Communication takes place in both direction and both systems can send information at the time.

TCP/IP - Transmission control protocol/Internet protocol

IP:

The main task is to support internetwork addressing and packet forwarding and routing.
Is a connectionless protocol that envelops data passed to it from the transport layer.

TCP:

Is a reliable and connection-oriented protocol, that ensures that packets are delivered to the destination computer.

If a packet is lost during transmission, TCP has the capability to resend it.

Provides reliability and ensures that the packets are delivered.

There is more overhead in TCP packet.

Data - Stream-> Segment -> Datagram -> Frame

UDP:

Is a best-effort and connectionless oriented protocol.

Does not have packet sequencing, flow and congestion control and the destination does not acknowledge every packet it receives.

There is less overhead in UDP packet.

Data - Message -> Packet -> Datagram -> Frame

TCP Handshake:

1. Host sends a SYN packet
2. Receiver answers with a SYN/ACK packet
3. Host sends an ACK packet

IPv4 - Uses 32 bits for its address

IPv6 - Uses 128 bits for its address

LAN media access technologies

Ethernet:

Characteristics: Share media / Uses broadcast and collision domains / Uses carrier sense multiple access with collision detection (CSMA/CD) access method / Supports full-duplex on twisted-pair implementations / Can use coaxial or twisted-pair media / Defined by standard 802.3

10base2 implementation: ThinNet, uses coaxial cable, maxlength 185 meters, provides 10 Mbps.

10base5 implementation: Thicknet, uses coaxial cable, maxlength 500 meters, provides 10 Mbps.

10base-T implementation: Uses twisted-pair wiring, provides 10 Mbps, usually implemented in star topology.

Fast Ethernet implementation: Uses twisted-pair wiring, provides 100 Mbps.

Token ring:

Uses a token-passing technology with a star configured topology.

Each computer is connected to a central hub, MAU - Multistation Access Unit.

Transmits data at 16 Mbps.

Active monitor - Removes frames that are continuously circulating on the network.

Beaconing - If a computer detects a problem with the network, it sends a beacon frame. It generates a failure domain where computers and devices will attempt to reconfigure certain settings to try and work around the detected fault.

FDDI—Fiber Distributed Data Interface:

Is a high speed token-passing media access topology.

Transmits data at 100 Mbps

Provides fault tolerance by providing a second counterrotating fiber ring.

Enables several tokens to be present on the ring at the same time.

Cabling

Coaxial Cable:

Is more resistant to EMI electromagnetic interference, provides a higher bandwidth and longer cable lengths compared to twisted pair.

Can transmit using a baseband method, where the cable carries only one channel

Can transmit using a broadband method, where the cable carries several channels.

Twisted pair:

Is cheaper and easier to work with than coaxial cable.

STP Shielded twisted pair - Has an outer foil shielding which is added protection from radio frequency interference.

UTP Unshielded twisted pair - Different categories of cabling that have different characteristics.

Fiber-optic cabling:

Because of the use of glass, it has higher transmission speeds that can travel over longer distances and is not affected by attenuation and EMI when compared to cabling that uses copper. It does not radiate signals like UTP cabling and is very hard to tap into.

Is expensive.

Cabling problems:

Noise - The receiving end will not receive the data in the form that was originally transmitted. Can be caused by motors, computers, copy machines, florescent lightning and microwave ovens.

Attenuation - The loss of signal strength as it travels or caused by cable breaks and cable malfunctions.

Crosstalk - When electrical signals of one wire spill over to another wire. UTP is much more vulnerable to this than STP or coaxial.

Plenum space - Network cabling that is placed in an area to meet specific fire rating to ensure that it will not produce and release harmful chemicals in case of a fire.

Pressurized conduits - Encapsulation of wires so if there is an attempt to access a wire, the pressure of the conduit will change and sound an alarm or send a message to the administrator.

Types of transmission

Analog transmission signals - Modulation of signals, electromagnetic waves.

Digital transmission signals - Represents binary digits as electrical pulses.

Asynchronous communication - Two devices are not synchronized in any way. The sender can send data at anytime and the receiving end must always be ready. Can be a terminal and a terminal server or modem.

Synchronous communication - Takes place between two devices that are synchronized, usually via a clocking mechanism. Transfers data as a stream of bits.

Baseband - Uses the full cable for its transmission

Broadband - Usually divides the cable into channels so that different types of data can be transmitted at a time.

Unicast method - A packet needs to go to one particular system

Multicast method - A packet need to go to a specific group of systems

Broadcast method - A packet goes to all computers on its subnet

Network Topology

Ring Topology:

Has a series of devices connected by unidirectional transmission links, that forms a ring.

Each node is dependent upon the preceding nodes and if one system failed, all other systems could fail.

Bus Topology:

A single cable runs the entire length of the network. Each node decides to accept, process or ignore the packet. The cable where all nodes are attached is a potential single point of failure.

Linear bus - Has a single cable with nodes attached to it.

Tree topology - Has branches from the single cable and each branch can contain many nodes.

Star Topology:

All nodes connect to a central hub or switch. Each node has a dedicated link to the central hub.

Mesh Topology:

All systems and resources are connected to each other in a way that does not follow the uniformity of the previous topologies.

LAN Media Access Technologies

MTU - Is a parameter that indicates how much data a frame can carry on a specific network.

Token passing:

Is a 24-bit control frame used to control which computers communicate at what intervals. The token grants a computer the right to communicate. Do not cause collisions because only one computer can communicate at a time.

CSMA Carrier sense multiple access:

CSMA/CD (collision detection) - Monitor the transmission activity or carrier activity on the wire so that they can determine when would be the best time to transmit data. Computers listen for the absence of a carrier ton on the cable, which indicates that no one else is transmitting date at the same time.

Contention - The nodes have to compete for the same shared medium

Collision - Happens when two or more frames collide.

Back-off algorithm - All stations will execute a random collision timer to force a delay before they attempt to transmit data.

CSMA/CA (collision avoidance) - Is an access method where each computer signals its intent to transmit data before it actually does so.

Collision Domains:

Is a group of computers that are contending or competing for the same shared communication medium.

Polling:

Some systems are configured to be primary stations and others are secondary stations. At predefined intervals, the primary station will ask the secondary station if it has anything to transmit.

Protocols

ARP - Knows the IP address and broadcasts to find the matching hardware address, the MAC address.

RARP - Knows the hardware address and broadcasts to find the IP address.

Masquerading attack - An attacker alter a system's ARP table so that it contains incorrect information (ARP table poisoning).

DHCP - A computer depends upon a server to assign it the right IP address.

BOOTP - Can receive a diskless computers IP address from a server

ICMP - Delivers messages, reports errors, replies to certain requests, reports routing information and is used to test connectivity and troubleshoot problems on IP networks.

Networking devices

Device	OSI Layer	Functionality
Repeater	Physical	Amplifies signals and extends networks.
Bridge	Data link	Forwards packets and filters based on MAC addresses; forwards broadcast traffic, but not collision traffic.
Router	Network	Seperates and connects LANs creating internetworks; routers filter based on IP addresses.
Brouter	Data link andNetwork	A hybrid device that combines the functionality of a bride and a router. A brouter can bridge multiple protocols and can route packets on some of those protocols.
Switch	Data link(More intelligent switches work at the network layer)	Provides a private virtual link between communicating devices, allows for VLANs, reduces traffic and impedes network sniffing.
Gateway	Application(although different types of gateways can work at otherLayers)	Connects different types of networks, performs protocol and format translations.

Comments on bridges:

Three types of bridges:

- Local bridge: Connects two or more LAN segments within a local area.
- Remote bridge: Can connect two or more LAN segment over a wide area network by using telecommunications.
- Translation bridge: If two LANs being connected are different types and use different standards and protocols.

Broadcast storm - Because bridges forward all traffic, the forward all broadcast packets.

STA Spanning Tree Algorithm - Ensures that frames do not circle networks forever, provides redundant paths in case a bridge goes down, assigns unique identifiers to each bridge, assigns priority values to these different bridges and calculates path costs.

Source routing - The packets hold the forwarding information so that they can find their way to the destination themselves without bridges and routers dictating their paths.

VLAN Virtual LANs:

Enable administrators to logically separate and group users based on resource requirements, security or business needs instead of the standard physical location of the users.

PBX Private Branch Exchange:

Is a telephone switch that is located on a company's property.

Firewalls

Restrict access from one network to another, internally or externally.

DMZ - Demilitarized Zone:

A Network segment that is located between the protected and the unprotected networks.

Packet filtering:

A method controlling what data can flow into and from a network.

Take place by using ACL's, which are developed and applied to a device.

Is based on network layer information, which means that the device cannot look too far into the packet itself.

Is not application dependent.

Do not keep track of the state of a connection.

Provides high performance.

Used in first-generation firewalls.

Stateful Packet Filtering:

It remembers and keeps track of what packets went where until that particular connection is closed. This requires the firewall to maintain a state table, which is like a score sheet of who said what to whom.

Make decisions on what packets to allow or disallow.

Works at the network layer.

Proxy firewalls:

Stands between a trusted and untrusted network and actually makes the connection, each way, on behalf of the source.

Makes a copy of each accepted packet before transmitting it and repackages the packet to hide the packet's true origin.

Works at the application layer

Dual-homed firewall:

Has two interfaces; one facing the external network and the other facing the internal network.

Has two NICs and has packet forwarding turned off.

Are often used when a company uses proxy firewalls.

Application-level proxies:

Inspect the entire packet and make access decisions based on the actual content of the packet.

Understand different services and protocols and the commands that are used within them

There must be one application-level proxy per service.

Works at the application level.

Circuit-level proxy:

Creates a circuit between the client computer and the server

It knows the source and destination addresses and makes access decisions based on this information.

Can handle a wide variety of protocols and services.

Works at the network layer.

SOCKS:

Is an example of a circuit-level proxy gateway that provides a secure channel between two TCP/IP computers.

Does not provide detailed protocol-specific control.

Firewall architecture

Bastion Host:

It is the machine that will be accessed by any and all entities trying to access or leave the network.

Can support packet filtering, proxy and hybrid firewall applications.

Screened Host:

Is a bastion host firewall that communicates directly with a border router and the internal network.

Screened Subnet:

The bastion host, housing the firewall, is sandwiched between two routers. The external applies packet filtering and the internal also filters the traffic.

Shoulds of Firewalls:

The default action of any firewall should be to implicitly deny any packets not explicitly allowed.

Masquerading / spoofing:

The attacker modifies a packet header to have the source address of a host inside the network that she wants to attack.

Honeypot:

Is a computer that sits in the DMZ in hopes to lure attackers to it instead of actual production computers.

Networking Services

NOS - Networking operations system:

Is designed to control network resource access and provide the necessary services to enable a computer to interact with the surrounding network.

DNS - Domain Name service:

Is a method of resolving hostnames.

Networks are split up into zones

The DNS server that holds the files for one of these zones is said to be the authoritative name server for that particular zone.

It is recommended that there be a primary and secondary DNS server for each zone.

Directory Services:

Has a hierarchical database of users, computers, printers, resources and attributes of each.

Intranets and Extranets

Intranets:

When a company uses Internet- or Web-based technologies inside their networks.

Extranets:

Enable two or more companies to share common information and resources.

NAT Network Address Translation:

Is a gateway between a network and the Internet, or another network, that performs transparent routing and address translation.

MAN - Metropolitan Area Network

Usually a backbone that connects businesses to WANs, the Internet and other businesses.

A majority are SONET / Synchronous Optical Network or FDDI rings.

WAN - Wide Area Network

Are used when communication needs to travel over a larger geographical area.

Dedicated links:

Also called leased line or point-to-point link.

T-carriers:

Dedicated lines that can carry voice and data information over trunk lines.

S/WAN - Secure WAN:

Based on VPNs that are created with IPSec.

WAN Technologies

CSU/DSU - Channel Service Unit / Data Service Unit:

Is required when digital equipment will be used to connect a LAN network to a WAN network.

DSU converts digital signals to be transmitted over the telephone company's digital lines.

CSU is the unit that connects the network directly to the telephone company's line.

Provides a digital interface for DTE - Data Terminal Equipment.

Provides an interface to the DCE - Data Circuit-Terminating Equipment device.

Switching:

Circuit switching - Sets up a virtual connection that acts like a dedicated link between two systems.

Packet switching - Packets can travel along many different routes to arrive to the same destination.

Frame relay:

Is a WAN protocol that operates at the data link layer.

Uses packet-switching technology.

CIR /committed information rate - Companies that pay more to ensure that a higher level of bandwidth will always be available to them.

Two main types of equipment used:

- DET / Data Terminal Equipment - Customer owned.
- DCE / Data Circuit-Terminating Equipment - Service provider's or phone company's

Virtual Circuits:

PVC / Permanent virtual circuit - Works like a private line for a customer with an agreed-upon bandwidth availability.

SVC / switched virtual circuits - Require steps similar to a dial-up and connection procedure.

X.25:

Is an older WAN protocol that defines how devices and networks establish and maintain connections.

Is a switching technology.

Data is divided into 128 bytes and encapsulated in High-level Data Link Control (HDLC) frames. The frames are then addressed, and forwarded across the carrier switches.

ATM - Asynchronous Transfer Mode:

Is a switching technology.

Uses a cell-switching technology. This means that data is segmented into fixed size cells, 53 bytes, instead of variable-size packets.

Is a high-speed networking technology used for LAN, WAN and service provider connections

Sets up virtual circuits, which act like dedicated paths between the source and destination.

These virtual circuits can guarantee bandwidth and QoS.

SMDS - Switched Multimegabit Data Service:

Is a high-speed packet-switched technology used to enable customers to extend their LANs across MANs and WANs

Is connectionless and can provide bandwidth on demand.

SDLC - Synchronous Data Link Control:

Is based on networks that use dedicated, leased lines with permanent physical connections.

Provides the polling media access technology, which is a mechanism that enables secondary stations to communicate on the network.

HDLC - High-level Data Link Control:

Is a bit-oriented link layer protocol used for transmission over synchronous lines.

Works with primary stations that contact secondary stations to establish data transmission.

HSSI - High-Speed Serial Interface:

Is used to connect multiplexers and routers to high-speed communication services like ATM and frame relay.

Multiservice Access:

Combine different types of communication categories over one transmission line.

Jittering - When someone using VoIP for phone call experiences lags in the conversation.

H.323:

Is a part of ITU-T recommendations that cover a wide variety of multimedia communication services.

Remote Access

Dial-up and RAS:

RAS / Remote Access Service server - Performs authentication by comparing the provided credentials with the database of credentials it maintains.

Wardialing - Is a process used by many attackers to identify remote access modems.

ISDN - Integrated Services Digital Network:

Breaks the telephone line into different channels and transmits data in a digital form versus the old analog method.

Three methods -

- BRI / Basic Rate Interface - 2 B channels and 1 D channel.

- PRI / Primary Rate Interface - 23 B channels and 1 D channel.

- BISDN / Broadband - Handle different types of services at the same time.

The D channel provides for a quicker call setup and process of making a connection.

DSL - Digital Subscriber Line:

Is a broadband technology.

The services can be symmetric -> Speed upstream <> downstream.

Connected all the time.

Cable modems:

Provide high speed access.

Connected all the time.

VPN - Virtual Private Network:

Is a secure private connection through a public network.

PPTP - Point-to-point tunnelling protocol:

Is an encapsulation protocol based on PPP.

Works at the data link layer and it enables a single point-to-point connection.

Encrypts and encapsulates PPP packets

When negotiating takes place, PPTP cannot encrypt this information because encryption is in the process of being invoked.

Can only work on top of IP networks

L2TP - Layer 2 Tunnelling Protocol:

Can run on top and tunnel through networks that use other protocol

Is not an encryption protocol.

Supports TACACS+ and RADIUS

L2F - Layer 2 Forwarding:

Provides mutual authentication

No encryption

IPSec:

Handles multiple connections at the same time

Provides secure authentication and encryption

Supports only IP networks

Focuses on LAN-to-LAN communication rather than a dial-up protocol

Works at the network layer and provides security on top of IP

Can work in tunnel mode, meaning the payload and header is encrypted or transport mode, meaning that only the payload is encrypted.

PPP - Point-to-Point:

Is used to encapsulate messages and transmit them through an IP network.

PAP - Password Authentication Protocol:

Provides identification and authentication of the user attempting to access a network from the remote system.

CHAP - Challenge Handshake Authentication Protocol:

Is an authentication protocol that uses challenge/response mechanism to authenticate instead of sending a username and password.

EAP - Extensible Authentication Protocol:

Provides a framework to enable many types of authentication techniques to be used during PPP connections.

Network and resource availability

Single point of failure:

If one device goes down, a segment or the entire network is negatively affected.

RAID - Redundant Array of Inexpensive Disks:

A technology used for redundancy and performance improvement that combines several physical disks and aggregates them into logical arrays.

Clustering:

A group of servers that are viewed logically as one server to users and are managed as a single system.

CBK#3 Security Management Practices

Fundamental Principles of Security

Security objectives -

Confidentiality:

Provides the ability to ensure that the necessary level of secrecy is enforced.

Integrity:

Is upheld when the assurance of accuracy and reliability of information and system is provided and unauthorized modification of data is prevented.

Availability:

Prevents disruption of service or productivity.

Definitions -

Vulnerability:

Is a software, hardware or procedural weakness that may provide the attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment.

Threat:

Is any potential danger to information or systems

Risk:

Is the likelihood of a threat agent taking advantage of a vulnerability.

Exposure:

Is an instance of being exposed to losses from a threat agent.

Countermeasure / safeguard:

Mitigates the potential risk.

Top-down approach:

The initiation, support and direction come from top management and work their way through middle management and then to staff members.

Bottom-up approach:

Security program developed by IT without getting proper management support and direction.

Operational goals:

Daily goals.

Tactical goals:

Mid-term goals.

Strategic goals:

Long-term goals.

Risk Management:

Is the process of identifying, assessing and reducing risks to an acceptable level and implementing the right mechanisms to maintain that level of risk.

Risk Analysis

Is a method of identifying risks and assessing the possible damage that could be caused in order to justify security safeguards.

Three main goals:

- identify risks
- quantify the impact of potential threats
- provide an economic balance between the impact of the risk and the cost of the countermeasure.

Risks have a loss potential: The company would lose something if a threat agent actually exploits a vulnerability.

Delayed loss: Has a negative effect on a company after a risk is initially exploited.

Quantitative Approach:

Attempts to assign real numbers to the costs of countermeasures and the amount of damage that can take place.

Provides concrete probability percentages when determining the likelihood of threats and risks.

Purely quantitative risk analysis is not possible because the method is attempting to quantify qualitative items.

Steps in risk analysis -

- Assign value to information and assets
- Estimate potential loss per risk
- Perform a threat analysis
- Derive the overall loss potential per risk
- Choose remedial measures to counteract each risk
- Reduce, assign or accept the risk

Calculating risks -

EF (Exposure Factor) = Percentage of asset loss caused by identified threat.

SLE (Single Loss Expectancy) = Asset value * Exposure Factor

ARO (Annualized Rate of Occurrence) = Estimated frequency a threat will occur within a year.

ALE (Annualized Loss Expectancy) = Single Loss Expectancy * Annualized Rate of Occurrence

Qualitative Approach:

Walk through different scenarios of risk possibilities and rank the seriousness of the threats and the sensitivity of the assets.

Procedures in performing the scenario:

- A scenario is written that addresses each major threat
- The scenario is reviewed by business unit managers for a reality check
- The RA team recommends and evaluates the various safeguards for each threat
- The RA team works through each finalized scenario using a threat, asset and safeguard.
- The team prepares their findings and submits them to management.

Delphie Technique:

Is a group decision method and is used to ensure that each member of a group gives an honest opinion of what he or she thinks the result to a particular risk will be.

Calculating countermeasures and risk:

Value of safeguard to the company = (ALE before implementing safeguard) - (ALE after implementing safeguard) - (annual cost of safeguard)

Total risk = threats * vulnerability * asset value

Residual risk = (threats * vulnerability * asset value) * control gap

Handling Risk:

Transfer risk -> Purchase an insurance

Reduce risk -> Implements countermeasures

Rejecting risk -> Denial of its risk or ignores it.

Accept the risk -> The company understands the level of risk they are under and the cost of damage that is possible and they decide to live with it.

Security Program

Categories of policy:

- Regulatory
- Advisory
- Informative

Security Policy:

Is a general statement produced by senior management to dictate what type of role security plays within the organization.

Are written in broad and overview terms to cover many subjects in a general fashion.

- Organisational security policy: Provides scope and direction for all further security activities within the organization.
- Issue-specific policies: Addresses specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply to these security issues.
- System-specific policy: Presents the management's decision that are closer to the actual computers, networks, applications and data.

Standards:

Specify how hardware and software products are to be used. They provide a means to ensure that specific technologies, applications, parameters and procedures are carried out in a uniform way across the organization.

These rules are usually compulsory within a company and they need to be enforced.

Baselines:

Provides the minimum level of security necessary throughout the organization.

Guidelines:

Are recommendation actions and operational guides to users, IT staff, operations staff and others when a specific standard does not apply.

Procedures:

Are step-by-step actions to achieve a certain task.

Procedures are looked at as the lowest level in the policy chain.

Data Classification

The primary purpose of data classification is to indicate the level of confidentiality, integrity and availability that is required for each type of information.

It helps to ensure that the data is protected in the most cost-effective manner.

Common classification levels (from highest to the lowest level):

Commercial business ->

- Confidential
- Private
- Sensitive
- Public

Military ->

- Top secret
- Secret
- Confidential
- Sensitive but unclassified
- Unclassified

Layers of Responsibility

Senior Manager:

Ultimately responsible for security of the organization and the protection of its assets.

Security professional:

Functionally responsible for security and carries out sensitive manager's directives.

Data Owner:

Is usually a member of senior management and is ultimately responsible for the protection and use of the data.

Decides upon the classification of the data he is responsible for and alters these classifications if the business needs arise.

Will delegate the responsibility of the day-to-day maintenance of the data, which is the responsibility of the data custodian.

Data Custodian:

Is given the responsibility of the maintenance and protection of the data.

User:

Any individual who routinely uses the data for work-related tasks.

Must have the necessary level of access to the data to perform the duties within her position and is responsible for following operational security procedures to ensure the data's C/I/A to others.

Structure and practices:

Separation of duties:

Makes sure that one individual cannot complete a risky task by herself.

Collusion:

More than one person would need to work together to cause some type of destruction or fraud and this drastically reduces its probability.

Nondisclosure agreements:

To protect the company if and when this employee leaves for one reason or another.

Job rotation:

No one person should stay in one position for a long period of time because it can end up giving too much control of a segment of the business to this one individual.

Security Awareness

Types of training:

- Security-related job training for operators
- Awareness training for specific departments or personnel groups with security sensitive positions
- Technical security training for IT support personnel and system administrators
- Advanced InfoSec training for security practitioners and information system auditors.

- Security training for senior managers, functional managers and business unit managers.

CBK#4 Applications & Systems Development Security

Database systems and database management

Types of databases:

- Hierarchical
- Mesh
- Object-oriented
- Relational

DBMS / Database Management System -

A suite of programs used to manage large sets of structured data with ad hoc query capabilities for many types of users

Database:

A collection of data stored in a meaningful way that enables multiple users and applications to access, view and modify data as needed.

Database terms/jargon -

- Record: Collection of related data items
- File: Collection of record of the same type
- Database: Cross-referenced collection of files
- DBMS: Manages and controls the database
- Base relation: A table stored in a database
- Tuple: A row in a database
- Attribute: A column in a database
- Primary key: Columns that make each row unique
- View: Virtual relation defined by the database to control subjects from viewing certain data
- Foreign key: Attribute of one table that is the primary key of another table
- Cell: Intersection of a row and column
- Schema: Holds data that describes a database
- Data dictionary: Central repository of data element and their relationships.
- Cardinality: The number of rows in the relation.
- Degree: The number of columns in the relation.
- Domain: Is a set of allowable values that an attribute can take.

Database models:

Relational data model -

Uses attributes (columns) and tuples (rows) to contain and organize information.

A primary key is a field that links all the data within a record to a corresponding value.

Hierarchical data model -

Combines records and fields that are related in a logical tree structure.

Can have one child, many children, no children.

Are useful for mapping one-to-many relationships.

Distributed data model -

Has data stored in more than one database, but it is logically connected.

Enable different databases to be managed by different administrators, although one person or group must manage the entire logical database.

Relational database components:

DDL / Data Definition Language -

Defines the structure and schema of the database.

- Structure: table size, key placement, views and data element relationships.
- Schema: the type of data that will be held and manipulated and their properties.

DML / Data Manipulation Language -

All the commands that enable a user to view, manipulate and use the database.

QL / Query Language -

Enables users to make requests of the database.

Report Generator -

Produces printouts of data in a userdefined manner.

Data dictionary:

Is a central repository of data elements and their relationships.

Is a collection of data elements, schema objects and reference keys.

Schema objects - Can contain tables, views, indexes, procedures, functions and triggers.

Keys:

Primary key -

Is a unique identifier in the table that unambiguously point to an individual tuple or row in the table.

Is a subset of candidate keys within a table.

Foreign key -

An attribute (column) in one relation that has values matching the primary key in another relation.

Integrity:

Concurrency problems -

Making sure that different subjects receive the most up-to-date information.

Semantic integrity -

Makes sure that structural and semantic rules are enforced. These rules pertain to data types, logical values, uniqueness constraints and operations that could adversely affect the structure of the database.

Referential integrity -

Mechanism would ensure that no record would contain a reference to a primary key of a nonexisting record or a NULL value.

Entity integrity -

If an attribute is NULL.

Rollback -

Is a statement that ends a current transaction and cancels all other changes to the database.

Commit -

Terminates a transaction and executes all changes that were just made by the user.

Checkpoint -

Are used to make sure that if a system failure occurs or if an error is detected, the user can always return to a point in time before the system crashed.

Database security issues:

Aggregation -

When a user does not have the clearance or permission to access specific information, but she does have the permission to access components of this information. She can then figure out the rest and obtain restricted information.

Inference -

Happens when a subject deduces information that is restricted from data he has access to. This is seen when data at a lower security level indirectly portrays data at a higher level.

Content-dependents access control -

Looks at the content of a file when it makes an access control decision. This type of access control increases processing overhead, but it provides higher granular control.

Cell suppression -

Is a technique used to hide or not show specific cells that contain information that could be used in inference attacks.

Partitioning -

Involves dividing the database into different parts, which makes it much harder for an unauthorized individual to find connecting pieces of data that can be brought together and other information that can be deduced or uncovered.

Noise and perturbation -

Is a technique of inserting bogus information in the hope of misdirecting an attacker or confusing the matter enough that the actual attack will not be fruitful.

Database views -

Permit one group or a specific user to see certain information, while restricting another group from viewing it altogether.

Polyinstantiation -

Enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level.

OLTP / On Line Transaction Processing -

Provides mechanisms that watch for problems and deal with them appropriately when they do occur.

- Two-phase commit service: Will make sure that a transaction is not complete until all databases receive and reflect a change

Data warehousing -

Combines data from multiple databases into a large database with the purpose of a fuller extent of information retrieval and data analysis

Data mining -

Is the process of messaging the data held in the data warehouse into more useful information.

- Metadata: Data produced by data mining tools to find associations and correlations.

OODB / Object-Oriented Data Bases -

Have the characteristics of ease of reusing code and analysis, reduced maintenance and an easier transition from analysis of the problem to design and implementation.

Its main disadvantages are a steep learning curve and high overhead of hardware and software required for development and operation.

Object-Relational Databases -

Combines the attributes of object-oriented and relational technologies.

System life cycle phases/software life cycle development process

System Life Cycle Phases:

- Project initiation:

- Conception of project definition

- Proposal and initial study

- Functional design analysis and planning

- Requirements uncovered and defined

- System environment specification determined

- System design specifications
 - Functional design review
 - Functionality broken down
 - Detailed planning put into place
 - Code design
- Software development
 - Developing and programming software
- Installation / implementation
 - Product installation
 - Testing and auditing
- Operational/maintenance
 - Product changes, fixes and minor modifications
- Disposal / Revision and replacement
 - Modifying the product with revisions or replacing it altogether

The Waterfall Model:

- System requirements
- Software requirements
- Analysis
- Program design
- Coding
- Testing
- Operations & Maintenance

Modified Waterfall Model incorporating V&V:

- System feasibility -> validation
- Software plans & requirements -> validation
- Product design -> verification
- Detailed design -> verification
- Coding -> unit test
- Integration Product -> verification
- Implementation -> system test
- Operations & Maintenance -> revalidation

Security concerns:

- Security should be addressed in each phase of system development. Security should not be addressed at the end of development because of the added cost, time, effort and lack of functionality.
- Separation of duties should be practiced in roles, environments and functionality pertaining to development of a product.
- A programmer should not have direct access to code in production.
- Certification deals with testing and assessing the security mechanism in a system
- Accreditation pertains to the management formally accepting the system and its security level.
- Changes must be authorized, tested and recorded. The changes must not affect the security level of the system or its capability to enforce the security policy.

Change control sub-phases:

- Request control
- Change control

- Release control

Change control process:

- Make a formal request of change
- Analyze the request
 - Develop the implementation strategy
 - Calculate the costs of this implementation
 - Review any security implications
- Record the change request
- Submit the change request for approval
- Develop the change
 - Recode segments of the product and add or subtract functionality.
- Link these changes in the code to the formal change control request
- Submit software for testing and quality approval
- Repeat until quality is adequate
- Make version changes

Configuration management:

- Configuration identification
- Configuration control
- Configuration status accounting
- Configuration audit

CMM / Software Capability Maturity Model

- Level 1: Initiating - Competent people and heroics; processes are informal and ad hoc
- Level 2: Repeatable - Project management processes; project management practices are institutionalized
- Level 3: Defined - Engineering processes and organizational support; technical practices are integrated with management practices institutionalized
- Level 4: Managed - Product and process improvement; product and process are quantitatively controlled
- Level 5: Optimized - Continuous process improvement; process improvement is institutionalized

Application Development Methodology

Types of languages:

Machine language: Is in a form that the computer and processor can understand and work with directly

Assembly language: Cannot be understood directly by the system and must be processed, which results into machine code language.

High-level language: Cannot be understood directly by the system and must be processed, which results into machine code language.

Programs:

Interpreted programs: Have instructions that are read and interpreted by a program one instruction at a time.

Compiled programs: Are written in a high-level language and turned into machinereadable format by a program called compiler.

OOP / Object-Oriented Programming:

Works with classes and objects within those classes.

Once the class is defined, the attributes can be reused for each new member or instance of the class that is created.

The object encapsulate the attribute values, which means that this information is packaged under one name and can be reused as one entity by other objects.

An object can have a shared portion - The interface that enables it to interact with other components

An object can have a private portion - How it actually works and performs the requested operations

Messages enter through the interface to specify the requested operation or method to be performed.

Information hiding - There is no need for other components to know how each object works internally.

Abstraction - Is the capability to suppress unnecessary details so that the important, inherent properties can be examined and reviewed

Phases of object-orientation:

OORA / Object-Oriented Requirements Analysis -

Defines classes of objects and their interactions.

OOA / Object-Oriented Analysis

In terms of object-oriented concepts, understanding and modelling a particular problem within a problem domain.

DA / Domain Analysis

Seeks to identify the classes and objects that are common to all applications within a given domain.

OOD / Object-Oriented Design

Object is the basic unit of modularity; objects are instantiations of a class.

OOP / Object-Oriented Programming

Emphasizes the employment of objects and methods rather than types or transformations as in other programming approaches.

Features of OOP:

Encapsulation - Hides internal data and operations.

Polymorphism - Makes copies of objects and makes changes to those copies.

Polyinstantiation - Multiple distinct differences between data within objects to discourage lower-level subjects from learning information at a higher-level of security.

Inheritance - Shares properties and attributes.

Multiple inheritance - Is the situation where a class inherits the behavioural characteristics of more than one parent class.

Delegation - Forwarding of a request by an object to another object or delegate. This forwarding is necessitated by the fact that the object receiving the request does not have a method to service the request.

Data Modelling:

Structured analysis approach:

Looks at all objects and subjects of an application and maps the interrelationships, communication paths and inheritance properties.

Data modelling:

Considers data independently of the way that the data is processed and the components that process the data.

Data Structures:

Data Structure:

Is a representation of the logical relationship between elements of data.

Cohesive:

A cohesive module can perform a single task with little or no help from other modules

- Low Cohesion: Scatter brained, does several tasks.
- High Cohesion: Focused on one task.

The best programming uses the most cohesive modules possible, but because different modules need to pass data and communicate, they usually cannot be totally cohesive.

Coupling:

Is a measure of interconnection among modules in an application.

- Low Coupling: Promotes module independence.
- High Coupling: Depend on other modules

The lower the coupling, the better the software design, because it promote module independence. The more independent a component is, the less complex the application is and the easier it is to modify and troubleshoot.

OMA / Object Management Architecture:

ORB / Object Request Brokers:

Manages all communication between components and enables them to interact in a heterogeneous and distributed environment.

CORBA / Common Object Request Broker Architecture:

Provides interoperability among the vast array of different software, platforms and hardware in environments.

Enables applications to communicate with one another no matter where the application is located or who developed it. To implement this compatible interchange, a user develops a small amount of initial code and an Interface Definition Language (IDL) file.

COM / Common Object Model:

Supports the exchange of objects among programs.

DCOM / Distributed Common Object Model:

Defines the standard for sharing objects in a networked environment.

Uses a globally unique identifier, GUID, to uniquely identify users, resources and components within an environment.

ODBC / Open Database Connectivity:

Provides a standard SQL dialect that can be used to access many types of relational databases.

DDE / Dynamic Data Exchange:

Enables different applications to share data by providing IPC.

Is a communication mechanism that enables direct conversation between two applications.

DCE / Distributed Computing Environment:

Is a set of management services with a communication layer based on RPC.

Is a layer of software that sits on top of the network layer and provides services to the applications above it.

Uses universal unique identifier, UUID, to uniquely identify users, resources and components within an environment.

The RPC function collects the arguments and commands from the sending program and prepares them for transmission over the network.

The DFS / Distributed File Services provides a single integrated file system that all DCE users can use to share files.

Expert systems / knowledge based systems:

Use artificial intelligence / emulate human knowledge to solve problems.

Is a computer program containing a knowledge base and set of algorithm and rules used to infer new facts from knowledge and incoming data.

- Rule-based programming: Is a common way of developing expert systems.
- Pattern matching: Based on if-then logic units.
- Inference engine: A mechanism that automatically matches facts against patterns and determines which rules are applicable.

Artificial Neureal Networks:

Is an electronic model based on the neural structure of the brain.

Tries to replicate the basic functions of neurons and their circuitry to solve problems in a new way.

Java:

Is a platform independent because it creates intermediate code, bytecode, which is not processor specific. The Java Virtual Machine then converts the bytecode to machine code. Java applets use a security scheme that employs a sandbox to limit the applet's access to certain specific areas within the user's system and protects them from malicious or poorly written applets.

ActiveX:

Microsoft technology that is used to write controls that Internet users can download to increase their functionality and Internet experience.

Practices security by informing the user where the program came from. Uses authenticode technology that relies on digital certificates and trusting certificate authorities.

Malicious Code:

Viruses, worms, trojan horses, logic bombs, ...

Can be detected by:

- File size increase
- Many unexpected disk accesses
- Change in update or modified timestamps

Virus:

Is a program that searches out other programs and infects them by embedding a copy of itself. When the infected program executes, the embedded virus is executed which propagates the infection.

- Boot sector virus: Move data within the boot sector or overwrite the sector with new information
- Stealth virus: Hides the modifications that it has made to files or boot records.
- Polymorphic virus: Produces varied but operational copies of itself.
- Multipart virus: Infects both the boot sector of a hard drive and executable files.

- Self-garbling virus: Attempts to hide from antivirus software by garbling its own code. As the virus spreads, it changes the way its code is encoded.

Worm:

They can reproduce on their own with no need for a host application and that they are self-contained programs.

Logic bomb:

Will execute a program, or string of code, when a certain event happens.

Trojan horse:

Is a program disguised as another program.

Attacks

DoS / Denial of Service:

An attack consuming the victim's bandwidth or resources, that cause the system to crash or stop processing other packet.

Smurf:

Requires three players: the attacker, the victim and the amplifying network.

The attacker spoofs, or changes the source IP address in a packet header, to make an ICMP ECHO packet seem as though it originated at the victim's system. This ICMP ECHO message is broadcasted to the amplifying network, which will reply to the message in full force. The victims system and victim's network is overwhelmed.

Fraggle:

Uses UDP as its weapon of choice. The attacker broadcasts a spoofed UDP packet to the amplifying network, which in turn replies to the victim's system

SYN Flood:

Continually sending the victim SYN messages with spoofed packets. The victim will commit the necessary resources to set up this communication socket and it will send its SYN/ACK message waiting for the ACK message in return.

Teardrop:

An attacker sending very small packets that would cause a system to freeze or reboot. Causes by the fact that some systems make sure that packets are not too large, but do not check to see if a packet is too small.

DDoS / Distributed Denial of Service:

Is a logical extension of the DoS.

The attacker creates master controllers that can in turn control slaves / zombie machines.

DNS DoS Attacks:

A record at a DNS server is replaced with a new record pointing at a fake/false IP address.

Cache poisoning - The attacker inserting data into the cache of the server instead of replacing the actual records.

CBK#5 Cryptography

Definitions

Algorithm: The set of mathematical rules used in encryption and decryption.

Cryptography: Science of secret writing that enables you to store and transmit data in a form that is available only to the intended individuals.

Cryptosystem: Hardware or software implementation of cryptography that transforms a message to ciphertext and back to plaintext.

Cryptoanalysis: Practice of obtaining plaintext from ciphertext without a key or breaking the encryption.

Cryptology: The study of both cryptography and cryptoanalysis.

Ciphertext: Data in encrypted or unreadable format.

Encipher: Act of transforming data into an unreadable format.

Decipher: Act of transforming data into a readable format.

Key: Secret sequence of bits and instructions that governs the act of encryption and decryption.

Key clustering: Instance when two different keys generate the same ciphertext from the same plaintext.

Keyspace: Possible values used to construct keys.

Plaintext: Data in readable format, also referred to as cleartext.

Work factor: Estimated time, effort, and resources necessary to break a cryptosystem.

Types of ciphers

Substitution cipher: Replaces bits, characters, or blocks of characters with different bits, characters or blocks.

Transposition cipher: Permutation is used, meaning that letters are scrambled. The key determines the positions that the characters are moved to.

Frequency analysis: Analysis of the frequent patterns of letters used in messages and conversation.

Running key cipher: Uses steps in the physical world around us, like books (page, line number and word count). Each word is described by a sequence of numbers.

Concealment cipher: Every X number of words within a text, is a part of the real message.

Steganography: Hiding data in another message so that the very existence of the data is concealed. A message can be hidden in a wave file, in a graphic or in unused spaces on a hard drive or sectors that are marked as unusable.

Clipper chip: A NSA designed tamperproof chip for encrypting data. Uses the SkipJack algorithm. Each Clipper Chip has a unique serial number and a copy of the unit key is stored in the database under this serial number. The sending Clipper Chip generates and sends a Law Enforcement Access Field (LEAF) value included in the transmitted message. Based on a 80-bit key and a 16-bit checksum.

Key Escrow: The unit keys are split into two sections and are given to two different escrow agencies to maintain.

Fair cryptosystems: Separate the necessary key required for decryption, but this method takes place in software encryption processes using public key cryptography, whereas key escrow is mainly used when hardware encryption chips are used.

Methods of Encryption

Symmetric Cryptography:

Both parties will be using the same key for encryption and decryption. Can only provide confidentiality. They are fast and can be hard to break.

Strength - Much faster than asymmetric systems / Hard to break if using a large key size

Weaknesses - Key distribution (requires a secure mechanism to deliver key properly) / scalability (each pair of users needs a unique pair of keys) / Limited security (can only provide confidentiality)

Out-of-band method: The key is transmitted through another channel than the message.

Asymmetric Algorithms:

Two different asymmetric keys are mathematically related, public and private key.

Strengths - Better key distribution than symmetric systems / better scalability than symmetric systems / can encrypt confidentiality, authentication and nonrepudiation

Secure message format - Encrypted by the receiver's public key

Open message format - Encrypted by the sender's private key

Secure and signed format - Encrypted by the senders private key and then encrypted with the receivers public key

Two types of symmetric algorithms

Stream ciphers:

Treats the message as a stream of bits or bytes and performs mathematical functions on them individually. The key is a random value input into the stream cipher, which it uses to ensure the randomness of the keystream data. Are more suitable for hardware implementations, because they encrypt and decrypt one bit at a time. Are intensive because each bit must be manipulated, which works better at the silicon level.

Characteristics of a strong and effective cipher algorithm - Long periods of no repeating patterns within keystream values / statistically unpredictable / the keystream is not linearly related to the key / statistically unbiased keystream (as many 0's as 1's)

Key stream generator - Produces a stream of bits that is XORed with the plaintext bits to produce ciphertext.

Block ciphers:

The message is divided into blocks of bits. Uses diffusion and confusion in their methods.

Uses Substitution boxes (S-boxes) In each step. It is the key that determines what functions are applied to the plaintext and in what order. Are more suitable for software implementations, because they work with blocks of data which is usually the width of a data bus (64 bits). Block ciphers sometimes work in a mode that emulates a stream cipher.

Confusion - Different unknown key values are used.

Diffusion - Putting the bits within the plaintext through many different functions so that they are dispersed throughout the algorithm.

S-box - Contains a lookup table that instructs how the bits should be permuted or moved around. The key that is used in the decryption process dictates what S-boxes are used and in what order.

Types of symmetric systems

Data Encryption Standard (DES):

Certified by NIST, based on IBM's 128 bit algorithm Lucifer. Is a block encryption algorithm. 64 bit in -> 64 bit out. 56 bits make up the true key and 8 bits are used for parity. A block of 64 bits is divided in half and each character is encrypted one at a time. The characters are put through 16 rounds of transposition and substitution functions. Have four distinct modes of operation:

ECB mode / Electronic Code Book - Native encryption mode. Provides the recipe of substitutions and permutations that will be performed on the block of plaintext. Data within a file does not have to be encrypted in a certain order. Used for small amounts of data, like challenge-response, key management tasks. Also used to encrypt PINs in ATM machines.

CBC mode / Cipher Block Chaining - Each block of text, the key, and the value based on the previous block is processed in the algorithm and applied to the next block of text.

CFB Mode / Cipher Feedback Mode - The previously generated ciphertext from the last encrypted block of data is inputted into the algorithm to generate random values. These random values are processed with the current block of plaintext to create ciphertext. This mode is used when encrypting individual characters is required.

OFB Mode / Output Feedback - Functioning like a stream cipher by generating a stream of random binary bits to be combined with the plaintext to create ciphertext. The ciphertext is fed back to the algorithm to form a portion of the next input to encrypt the next stream of bits.

DEA - Data Encryption Algorithm

FIPS - Federal Information Processing Standard

Trippel-DES (3DES):

Uses 48 rounds in its computation. Heavy performance hit and it can take up to three times longer than DES to perform encryption and decryption.

Advanced Encryption Standard (AES):

NIST replacement standard for DES. The winner was Rijndael, which is a block cipher with a variable block length and key length

Employs a round transformation that is comprised of three layers of distinct and invertible transformations: The non-linear layer / the linear mixing layer / the key addition layer. Is suited for high speed chips with no area restrictions / a compact co-processor on a smart card.

International Data Encryption Algorithm (IDEA):

Block cipher that operates on 64 bit blocks of data. The key is 128 bits long. The 64-bit data block is divided into 16 smaller blocks and each has eight rounds of mathematical functions performed on it. Is used in the PGP encryption software.

Blowfish:

A block cipher that works on 64-bit blocks of data. The key length can be up to 448 bits and the data blocks go through 16 rounds of cryptographic functions.

RC5:

A block cipher that has a variety of parameters it can use for block size, key size and the number of rounds used. Block sizes: 32/64/128 and key size up to 2048 bits.

Types of asymmetric systems

RSA:

Provides authentication (digital signature) and encryption. The security comes from the difficulty of factoring large numbers, where the keys are functions of a pair of large prime numbers.

Is used in many web browsers with SSL, in PGP and government system that use public key cryptosystems.

El Gamal:

Used for digital signatures and key exchange. Based on calculating discrete logarithms in a finite field.

Elliptic Curve Cryptosystem (ECC):

Provides digital signatures, secure key distribution and encryption. Requires smaller percentage of the resources than other systems. Based on the properties of elliptic curves in their public key system.

Hybrid Encryption Methods

Public Key Cryptography

Uses two keys generated by an asymmetric algorithm for protecting encryption keys and key distribution and a secret key is generated by a symmetric algorithm and used for bulk encryption.

- Asymmetric algorithm performs encryption and decryption by using public and private keys.
- Symmetric algorithm performs encryption and decryption by using a secret key.
- A secret key is used to encrypt the actual message
- A secret key is synonymous to a symmetric key
- An asymmetric key refers to a public or private key.

Diffie-Hellman Key Exchange

Were the first to introduce the notion of public key cryptography. Is used for key distribution and it cannot be used to encrypt and decrypt messages.

Session keys

Is a secret key that is used to encrypt messages between two users. Is only valid for one session.

Symmetric versus Asymmetric Systems

Attributes	Symmetric	Asymmetric
Keys	One key is shared between two or more entities.	One entity has a public key and the other entity has a private key.
Key exchange	Out-of-band.	Symmetric key is encrypted and sent with message; thus, the key is distributed by inbound means.
Speed	Algorithm is less complex and faster.	Algorithm is more complex and slower.
Key length	Fixed-key length	Variable-key length
Use	Bulk encryption, which means encrypting files and communication paths.	Key encryption and distributing keys.
Security service provided	Confidentiality and integrity	Confidentiality, integrity, authentication and non-repudiation

Public Key Infrastructure (PKI)

Digital certificate - A credential that contains the public key of that individual along with other identifying information.

Certificate authority (CA) - An organization that maintains and issues public key certificates.

Certificate revocation list (CRL) - A list of every certificate that has been revoked for one reason or another. This list is maintained periodically.

Certificate - Is the mechanism used to associate a public key with a collection of components sufficient to uniquely authenticate the claimed owner.

Registration authority (RA) - Performs the certification registration duties.

PKI entities and function - CA / RA / certificate repository / certificate revocation system / key backup and recovery system / automatic key update / management of key histories / cross-certification with other CAs / timestamping / client-side software
PKI supplies - Confidentiality / Access control / Integrity / Authentication

One-way function

Is a mathematical function that is easier to compute in one direction than in the opposite direction.

Trapdoor one-way function - The basis for public key cryptography. A public key encrypts and a private key (trapdoor) decrypts

Message integrity

One-way hash

Is a function that takes a variable-length string a message, and compresses and transforms it into a fixed length value referred to as a hash value.

Message digest - The hash value of a one-way hash.

One-way function used in public key cryptography

Function - It never performed in reverse / It provides integrity of a message, not confidentiality or authentication. / The result of a one-way hash is a hashing value / It is used in hashing to create a fingerprint for a message.

Digital signatures

Is an encrypted hash value of a message

Digital signature standard (DSS)

A standard for digital signatures and its functions and acceptable use. Require Digital Signature Algorithm (DSA) and the Secure Hash Algorithm (SHA).

Different Hash algorithm

MD4 - Produces 128-bit hash values. Used for high-speed computation in software implementation and is optimized for microprocessors.

MD5 - Produces 128-bit hash values. More complex than MD4. Processes text in 512-bit blocks.

MD2 - Produces 128-bit hash values. Slower than MD4 and MD5

SHA - Produces 160-bit hash values. This is then inputted into the DSA, which computes the signature for a message. The message digest is signed instead of the whole message.

SHA1—Updated version of SHA.

HAVAL - Is a variable length one-way hash function and is the modification of MD5. Processes text in 1024-bit blocks.

Attacks against one-way hash functions

Collision - If the algorithm does produce the same value for two distinctly different messages.

Birthday attack - Is an attack on hashing functions through brute force. The attacker tries to find two messages with the same hashing value

One-time pad

Is unbreakable and each pad is used exactly once

Uses a truly nonrepeating set of random bits that are combined bit-wise XOR with the message to produce ciphertext.

The random key is the same size as the message and is only used once.

Difficult to distribute the pads of random numbers to all the necessary parties.

Key Management

Kerberos - A key distribution center (KDC) is used to store, distribute and maintain cryptographic session keys.

Diffie-Hellman - Uses a key exchange algorithm (KEA)

Key Management principles:

Should not be in cleartext outside the cryptographic device.

Backup copies should be available and easily accessible when required.

A company can choose to have multiparty control for emergency key recovery. This means that if a key needs to be recovered, more than one person is required to be involved with this process.

Rules for key and key management:

- The key length should be long enough to provide the necessary level of protection.
- Keys should be stored and transmitted by secure means.
- Keys should be extremely random and use the full spectrum of the keyspace.
- The key's lifetime should correspond with the sensitivity of the data it is protecting.
- The more the key is used, the shorter its lifetime should be.
- Keys should be backed up or escrowed in case of emergencies.
- Keys should be properly destroyed when their lifetime comes to an end.

Link versus end-to-end encryption

Link encryption

Encrypts all the data along a specific communication path like a satellite link, T3 line or telephone circuit.

User information, header, trailers, addresses and routing data that are part of the packets are encrypted.

Provides protection against packet sniffers and eavesdroppers.

Packets have to be decrypted at each hop and encrypted again.

Is at the physical level.

End-to-end encryption

Only information is encrypted.

Is usually initiated at the application layer of the originating computer.

Stays encrypted from one end of its journey to the other.

Higher granularity of encryption is available because each application or user can use a different key.

E-mail standards

Privacy-enhanced mail (PEM):

Provide authentication, message integrity, encryption and key management.

Specific components that can be used:

- Messages encrypted with DES in CBC mode
- Authentication provided by MD2 or MD5
- Public key management provided by RSA
- X.509 standard used for certification structure and format

Message Security Protocol (MSP):

Can sign and encrypt messages and perform hashing functions.

Pretty Good Privacy (PGP):

First widespread public key encryption program

Uses RSA public key encryption for key management and IDEA symmetric cipher for bulk encryption of data.

PGP uses passphrases, that is used to encrypt the user's private key that is stored on her hard drive.

Relies on a "web of trust" in its key management approach.

Key ring - Each user keeps a collection of signed public keys he has received from other users.

Internet Security

HTTP:

Sits on the top of TCP/IP

Is a stateless protocol, client and web server make and break a connection for each operation.

S-HTTP - Secure Hypertext Transport Protocol:

Developed to provide secure communication.

Encrypts messages with session keys that are calculated.

Provides integrity and sender authentication capabilities.

Is not a stateless protocol

Can support multiple encryption modes and types.

Can use public key technology and symmetric encryption.

Used when an individual message needs to be encrypted.

HTTPS:

Protects the communication channel between two computers.

Uses SSL and HTTP to provide a protected circuit between a client and server.

Used when all information that passes between two computers needs to be encrypted.

SSL - Secure Sockets Layer:

Protects a communication channel.

Uses public key encryption.

Provides data encryption, server authentication, message integrity and optional client authentication.

Keeps the communication path open until one of the parties requests to end the session.

Lies beneath the application layer and above the transport layer.

MIME - Multipurpose Internet Mail Extension:

Indication how multimedia data and e-mail attachments are to be transferred.

S/MIME - Secure MIME:

Standard for encrypting and digitally signing electronic mail that contains attachments and providing secure data transmissions.

Provides confidentiality through the user's encryption algorithm, integrity through the user's hashing algorithm, authentication through the use of X.509 public key certificates and non-repudiation through cryptographically signed messages.

SET - Secure Electronic Transaction:

Developed to send encrypted credit card numbers

Comprised of three main parts: the electronic wallet, the software running on the merchant's server at its web site and the payment server that is located at the merchant's bank.

Cookies:

Text files that a browser maintains on a user's hard drive.

Are used for demographic and advertising information

Are used as timestamps to ensure that a session between a user and a server is restricted to a specific length of time.

Cookies that contain sensitive information should be encrypted by the server on the site that distributed them.

SSH - Secure Shell:

Functions as a type of tunnelling mechanism that provides terminal like access to remote computers.

Should be used instead of telnet, ftp, rlogin, rexec or rsh.

Two computers go through a handshake and a secure channel is established.

IPSec - Internet Protocol Security:

A method of setting up a secure channel for protected data exchange between two devices.

Widely accepted standard for secure network layer transport.

Have strong encryption and authentication methods that employ public key cryptography.

Is usually used to establish VPN.

It is an open, modular framework that provides a lot of flexibility.

Have two basic security protocols:

- AH - Authentication Header: Is the authenticating protocol.
- ESP - Encapsulating Security Payload: Is an authenticating and encrypting protocol that uses cryptographic mechanism to provide source authentication, confidentiality and message integrity.

Can work in two modes:

- Transport mode: The payload of the message is encrypted
- Tunnel mode: The payload, the routing and header information of the message is encrypted

SA - Security association - Can contain the authentication and encryption keys, the agreed upon algorithms, key lifetime and the source IP address. One SA for each connection.

SPI - Security parameter index - An index that keeps track of the different SAs and tells the device which one is appropriate to invoke.

ISAKMP - Internet Security Association and Key Management Protocol - An authentication and key exchange architecture that is independent of the type of keying mechanisms used.

Attacks

Ciphertext-only attack:

The attacker has the ciphertext of several messages. Each of the messages has been encrypted using the same encryption algorithm.

Known-plaintext only:

The attacker has the plaintext and ciphertext of one or more messages.

Chosen-plaintext attack:

The attacker has the plaintext and ciphertext and can choose the plaintext that gets encrypted.

Chosen-ciphertext attack:

The attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext.

Man-in-the-middle attack:

Eavesdropping on different conversations. Using digital signatures during the session-key exchange can circumvent the attack.

Dictionary attacks:

Takes a password file with one-way function values and then takes the most commonly used passwords and run them through the same one-way function. These files are then compared.

Replay attack:

An attacker copies a ticket and breaks the encryption and then tries to impersonate the client and resubmit the ticket at a later time to gain unauthorized access to a resource.

CBK#6 Security Architecture & Models

Security Model

Is a statement that outlined the requirements necessary to properly support a certain security policy.

Computer Architecture

CPU - Central Processing Unit:

Is a microprocessor

Contains a control unit, an ALU / Arithmetic Logic Unit and primary storage.

Instructions and data are held in the primary storage unit needed by the CPU.

The primary storage is a temporary memory area to hold instructions that are to be interpreted by the CPU and used for data processing.

Buffer overflow - Data being processed is entered into the CPU in blocks at a time. If the software instructions do not properly set the boundaries for how much data can come in as a block, extra data can slip in and be executed.

Real storage - As instructions and data are processed, they are moved back to the system's memory space / real storage.

Memory:

RAM / Random Access Memory - Is a volatile memory, because when power is lost -> information is lost.

Types of ram:

- Static RAM - When it stores data, it stays there without the need of being continually refreshed.

- Dynamic RAM - Requires that that data held within it be periodically refreshed because the data dissipates and decays.

ROM / Read-only memory - Is a nonvolatile memory. Software that is stored within ROM is called firmware.

EPROM / Erasable and programmable read-only memory - Holds data that can be electrically erased or written to.

Cache memory:

Is a part of RAM that is used for high-speed writing and reading activities.

PLD - Programmable Logic Device:

An integrated circuit with connections or internal logic gates that can be changed through programming process.

Memory Mapping:

Real or primary memory - Memory directly addressable by the CPU and used for the storage of instructions and data associated with the program that is being executed.

Secondary memory - Is a slower memory (such as magnetic disks) that provides non-volatile storage.

Sequential memory - Memory from which information must be obtained by sequential searching from the beginning rather than directly accessing the location (magnetic tape, ...)

Virtual memory - Uses secondary memory in conjunction with primary memory to present a CPU with a larger, apparent address space of the real memory locations.

Memory addressing:

Register addressing - Addressing the registers within a CPU or other special purpose registers that are designated in the primary memory.

Direct addressing - Addressing a portion of primary memory by specifying the actual address of the memory location. The memory addresses are usually limited to the memory page that is being executed or page zero.

Absolute addressing - Addressing all of the primary memory space.

Indexed addressing - Developing a memory address by adding the contents of the address defined in the program's instruction to that of an index register. The computed, effective address is used to access the desired memory location. Thus, if an index register is incremented or decremented, a range of memory location can be accessed.

Implied addressing - Used when operations that are internal to the processor must be performed such as clearing a carry bit that was set as a result of an arithmetic operation. Because the operation is being performed on an internal register that is specified within the instruction itself, there is no need to provide an address.

Indirect addressing - Addressing where the address location that is specified in the program instruction contains the address of the final desired location.

CPU Modes and Protection Rings:

Protection rings - Provide strict boundaries and definitions on what the processes that work within each ring can access and what commands they can successfully execute. The processes that operate within the inner rings have more privileges, privileged / supervisor mode, than the processes operating in the outer rings, user mode.

Operating states:

Ready state - An application is ready to resume processing.

Supervisory state - The system is executing a system, or highly privileged, routine.

Problem state - The system is executing an application.

Wait state - An application is waiting for a specific event to complete, like the user finishing typing in characters or waiting for a print job to finish.

Multi-threading, -tasking, -processing:

Multithreading - One application can make several calls at one time, that use different threads.

Multitasking - The CPU can process more than one process or task at one time.

Multiprocessing - If a computer has more than one CPU and can use them in parallel to execute instructions.

Input/Output Device Management:

Deadlock situation - If structures are not torn down and released after use. Resources should be used by other programs and processes.

System architecture

TCB - Trusted Computing Base:

Is defined as the total combination of protection mechanisms within a computer system.

Includes hardware, software and firmware.

Originated from the Orange Book.

The Orange Book defines a trusted system as hardware and software that utilize measures to protect the integrity of unclassified or classified data for a range of users without violating access rights and the security policy. It looks at all protection mechanisms within a system to enforce the security policy and provide an environment that will behave in a manner expected of it.

Security perimeter:

Defined as resources that fall outside of TCB.

Communication between trusted components and untrusted components needs to be controlled to ensure that confidential information does not flow in an unintended way.

Reference monitor:

Is an abstract machine, which mediates all access subjects have to objects to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification.

Is an access control concept, not an actual physical component.

Security kernel:

Is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.

Is the core of the TCB and is the most commonly used approach to building trusted computing systems.

Three requirements:

- It must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
- The reference monitor must be invoked for every access attempt and must be impossible to circumvent. Thus, the reference monitor must be implemented in a complete and foolproof way.
- It must be small enough to be able to be tested and verified in a complete and comprehensive manner.

Domains:

Defined as a set of objects that a subject is able to access.

Execution Domain - A program that resides in a privileged domain needs to be able to execute its instructions and process its data with the assurance that programs in a different domain cannot negatively affect its environment.

Security Domain - Has a direct correlation to the protection ring that a subject or object is assigned to. The lower the protection ring number, the higher the privilege and the larger the security domain.

Resource isolation:

Hardware segmentation - Memory is separated physically instead of just logically.

Security policy:

Is a set of rules, practices and procedures dictating how sensitive information is managed, protected and distributed.

Multilevel security policy - Security policies that prevent information from flowing from a high security level to a lower security level.

Least privilege:

Means that a resource, process has no more privileges than necessary to be able to fulfil its functions.

Layering:

A structured and hierarchical architecture that has the basic functionality taking place at lower layers and more complex functions at the higher layers.

Data hiding:

When it is required that processes in different layers do not communicate, therefore, they are not supplied with interfaces to interact with each other.

Abstraction:

When a class of objects is assigned specific permissions and acceptable activities are defined. This makes management of different objects easier because classes can be dealt with instead of each and every individual object.

Security Models

Maps the abstract goals of the policy to information systems terms by specifying explicit data structures and techniques necessary to enforce the security policy.

State machine model:

To verify the security of a system, the state is used, which means all current permissions and all current instances of subjects accessing objects must be captured.

State transitions - Activities that can alter a state.

A system that has employed a state machine model will be in a secure state in each and every instance of its existence. It will boot up into a secure state, execute commands and transactions securely, and will allow subjects to access resources only in secure states.

Bell-Lapuda model:

Address concerns about system security and leakage of classified information.

Multilevel security system - A system that employs the Bell-Lapuda model, where users with different clearances use the systems and the systems process data with different classifications.

The level at which information is classified determines the handling procedures that should be used -> forms a lattice.

Lattice - Is an upper bound and lower bound of authorized access.

Is a state machine model enforcing the confidentiality aspects of access control.

An access control matrix and security levels are used to determine if subjects can access different objects.

The model uses subjects, objects, access operations (read, write and read/write) and security levels.

Continued ... Bell-Lapuda model:

Is an information flow security model, which means that information does not flow to an object of lesser or noncomparable classification.

Two main rules:

- The simple security rule - A subject at a given security level cannot read data that resides at a higher security level. Is referred to no "read up" rule.

- *-property - States that a subject in a given security level cannot write information to a lower security level. Is referred to no "write down" rule.

Defines a secure state as a secure computing environment and the allowed actions which are security-preserving operations.

Basic Security Theorem - If a system initializes in a security state and all state transitions are secure, then every subsequent state will be secure no matter what inputs occur.

The model provides confidentiality, and does not address integrity of the data the system maintain.

Biba model:

Is an information flow model, concerned about data flowing from one security level to another.

Uses a state machine model.

Address the integrity of data being threatened when subject can read data at lower levels.

Prevents data from any integrity level from flowing to a higher integrity level.

Two main rules:

- "No write up" - A subject cannot write data to an object at a higher integrity level.
- "No read down" - A subject cannot read data from a lower integrity level.

Clark-Wilson model:

Protecting the integrity of information by focusing on preventing authorized users from making unauthorized modifications of data, fraud, and errors within commercial applications. Users cannot access and manipulate objects directly, but must access the object through a program.

Uses also separation of duties, which divides an operation into different parts and requires different users to perform each part. This prevents authorized user from making unauthorized modifications to data, which again protects its integrity.

Auditing is also required to track the information coming in from the outside of the system.

Information flow model:

Can deal with any kind of information flow, not only the direction of the flow.

Looks at insecure informational flow that can happen at the same level and between objects along with the flow between different levels.

A system is secure if there is no illegal information flow permitted.

Non interference Model:

Ensure that any actions that take place at a higher security level do not affect, or interfere, with actions that take place at a lower level

Security Modes of Operation

Dedicated Security Mode:

If all users have the clearance or authorization and need-to-know to all data processed within the system.

All users have been given formal access approval for all information on the system and have signed nondisclosure agreements pertaining to this information.

The system can handle a single classification level of information.

System-High Security Mode:

All users have a security clearance or authorization to access the information but not necessarily a need-to-know for all the information processed on the system (only some of the data).

Require all users to have the highest level of clearance, but a user is restricted via the access control matrix.

Compartmented Security Mode:

All users have the clearance to access all the information processed by the system, but might not have the need-to-know and formal access approval.

Users are restricted to being able to access some information because they do not need to access it to perform the functions of their jobs and they have not been given formal approval to access this data.

Compartments are security levels with limited number of subjects cleared to access data at each level.

CMW / Compartments - Enable users to process multiple compartments of data at the same time, if they have the necessary clearance.

Multilevel Security Mode:

Permits two or more classification levels of information to be processed at the same time when all the users do not have the clearance of formal approval to access all the information being processed by the system.

Trust and Assurance:

Trust - Tells the customer how much he can expect out of this system, what level of security it will provide.

Assurance - The system will act in a correct and predictable manner in each and every computing situation.

System Evaluation Methods

Examines the security-relevant parts of a system, meaning the TCB, access control mechanisms, reference monitor, kernel, protection mechanisms.

The Orange Book / TCSEC:

TCSEC - Trusted Computer System Evaluation Criteria.

Evaluates products to assess if they contain the security properties they claim and evaluate if the product is appropriate for a specific application or function.

Looks at the functionality, effectiveness and assurance of a system during its evaluation and it uses classes that were devised to address typical patterns of security requirements.

Focuses on the operating system.

Continued ... The Orange Book / TCSEC:

Hierarchical division of security levels -

A - Verified protection

B - Mandatory protection

C - Discretionary protection

D - Minimal security

Topics - Security policy, accountability, assurance and documentation

Areas -

Security policy - Must be explicit and well defined and enforced by the mechanisms within the system.

Identification - Individual subjects must be uniquely identified.

Labels - Access control labels must be associated properly with objects.

Documentation - Includes test, design, specification documents, user guides and manuals.

Accountability - Audit data must be captured and protected to enforce accountability.

Life cycle assurance - Software, hardware and firmware must be able to be tested individually to ensure that each enforces the security policy in an effective manner throughout its lifetime.

Continuous protection - The security mechanisms and the system as a whole must perform predictably and acceptably in different situations continuously.

Evaluation levels -

- D - Minimal Protection
- C1 - Discretionary Security Protection
- C2 - Controlled Access Protection
- B1 - Labeled Security
- B2 - Structured Protection
- B3 - Security Domains
- A1 - Verified Design

The Red Book / TNI:

TNI - Trusted Network Interpretation.

Addresses security evaluation topics for networks and network components.

It addresses isolated local area networks and wide area internetwork systems.

Security items addressed:

- * Communication integrity
 - Authentication
 - Message integrity
 - Nonrepudiation
- * Denial of service prevention
 - Continuity of operations
 - Network management
- * Compromise protection
 - Data confidentiality
 - Traffic flow confidentiality
 - Selective routing

Ratings -

- None
- C1 - Minimum
- C2 - Fair
- B2 - Good

ITSEC:

ITSEC - Information Technology Security Evaluation Criteria.

Only used in Europe

Two main attributes - Functionality and Assurance.

Is a criteria for both security products and security systems and refers to both as the target of evaluation (TOE).

Common Criteria:

Is an international evaluation standard.

EAL - Evaluation assurance level.

Protection profile - The set of security requirements, their meaning and reasoning and the corresponding EAL rating.

Two main attributes - Functionality and Assurance.

Five sections of the protection profile -

- Descriptive elements
- Rationale
- Functional requirements

- Development assurance requirements
- Evaluation assurance requirements

Certification <-> Accreditation

Certification:

Is the technical evaluation of the security components and their compliance for the purpose of accreditation.

Is the process of assessing the security mechanisms and controls and evaluating their effectiveness.

Accreditation:

Is the formal acceptance of the adequacy of a system's overall security by the management.

Is management's official acceptance of the information in the certification process findings.

Open Systems <-> Closed Systems

Open Systems:

Have an architecture that has published specifications, which enables third-party vendors to develop add-on components and devices.

Provides interoperability between products by different vendors of different operating systems, applications and hardware devices.

Closed Systems:

Use an architecture that does not follow industry's standards.

Interoperability and standard interfaces are not employed to enable easy communication between different types of systems and add-on features.

Are proprietary, meaning that the system can only communicate with like systems.

Threats to Security Models and Architectures

Covert Channels:

Is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism.

Covert timing channel - One process relays information to another by modulating its use of system resources.

Covert storage channel - When a process writes data to a storage location and another process directly or indirectly reads it. The problem occurs when the processes are at different security levels, and therefore not supposed to be sharing sensitive data.

- Countermeasures:

There is not much a user can do to countermeasure these channels.

For trojan horses that uses HTTP, intrusion detection and auditing may detect a covert channel.

Back Doors:

Also called maintenance hooks.

Are instructions within software that only the developer knows about and can invoke.

- Countermeasures:

Code reviews and unit and integration testing should always be looking out for back doors.

Preventative measures against back doors -

- Host intrusion detection system

Use File system permissions to protect configuration files and sensitive information from being modified.

Strict access control.
File system encryption.
Auditing

Timing Issues:

Also called asynchronous attack.

Deals with the timing difference of the sequences of steps a system uses to complete a task.
A time-of-check versus time-of-use attack, also called race conditions, could replace
autoexec.bat.

- Countermeasures:

Host intrusion detection system
File system permissions and encryption
Strict access control measures
Auditing

Buffer Overflows:

Sometimes referred to "smashing the stack"

When programs do not check the length of data that is inputted into a program and then
processed by the CPU.

- Countermeasures

Proper programming and good coding practices.
Host intrusion detection system
File system permission and encryption
Strict access control
Auditing

CBK#7 Operations Security

Controls and Protections

To protect hardware, software and media resources from:

- Threats in an operating environment
- Internal or external intruders
- Operators who are inappropriately accessing resources

Categories of Controls:

- Preventative Controls:

Are designed to lower the amount and impact of unintentional errors that are entering the system and to prevent unauthorized intruder from internally or externally accessing the system.

- Detective Controls:

Are used to detect an error once it has occurred.

- Corrective Controls / Recovery Controls:

Are implemented to mitigate the impact of a loss event through data recovery procedures.

- Deterrent Controls / Directive Controls:

Are used to encourage compliance with external controls.

- Application Controls:

Are the controls that are designed into a software application to minimize and detect the software's operational irregularities.

- Transaction Controls:

Are used to provide control over the various stages of a transaction. Types of controls are: Input, processing, output, change and test controls.

Orange Book Controls:

Operational assurance:

- System architecture
- System integrity
- Covert channel analysis
- Trusted facility management
- Trusted recovery

Life cycle assurance:

- Security testing
- Design specification and testing
- Configuration management
- Trusted distribution

Covert channel analysis:

- B2:

The system must protect against covert storage channels. It must perform covert channel analysis for all covert storage channels.

- B3 and A1:

The system must protect against both covert storage and covert timing channels. It must perform a covert channel analysis for both types.

Trusted Facility Management:

- B2:

Systems must support separate operator and system administrator roles.

B3 and A1:

System must clearly identify functions of the security administrator to perform the security-related functions.

Separation of duties and job rotation:

- Least privilege:

Means that a system's user should have the lowest level of rights and privileges necessary to perform their work and should only have them for the shortest length of time.

- Two-man control:

Two operators review and approve the work of each other, to provide accountability and to minimize fraud in highly sensitive or high-risk transactions.

- Dual control:

Both operators are needed to complete a sensitive task.

- Job rotation:

The process of limiting the amount of time an operator is assigned to perform a security related task before being moved to a different task with a different security classification.

Trusted Recovery:

Ensures that security is not breached when a system crash or other system failure occurs.

Is only required for B3 and A1 level systems.

- Failure preparation:

Backing up all critical files on a regular basis.

- System recovery

In common criteria three hierarchical recovery types -

- Manual recovery
- Automated recovery
- Automated recovery without undue Loss

Configuration / Change Management Control:

Procedures to implement and support change control process:

- Applying to introduce a change
- Cataloging the intended change
- Scheduling the change
- Implementing the change
- Reporting the change to the appropriate parties

Clipping Levels:

Thresholds for certain types of errors or mistakes allowed and the amount of these mistakes that can take place before it is considered suspicious. Once the clipping level has been exceeded, further violations are recorded for review.

Administrative Controls:

Controls that are installed and maintained by administrative management to help reduce the threat or impact of violations on computer security.

- Personal Security
 - Employment Screening or Background Checks
 - Mandatory Taking of Vacation in One Week Increment
 - Job Action Warnings or Termination
- Separation of Duties and Responsibilities

- Least Privilege
- Need to Know
- Change/Configuration Management Controls
- Record Retention and Documentation

Record Retention:

Data Remanence -

Refers to the data left on the media after the media has been erased

Operations Controls:

Day-to-day procedures used to protect computer operations.

Resource Protection:

Is the concept of protecting an organization's computing resources and assets from loss or compromise. Covers hardware, software and data resources.

Hardware Controls:

- Hardware Maintenance
- Maintenance Accounts
- Diagnostics Port Control
- Hardware Physical Control

Software Controls:

- Anti-virus Management
- Software Testing
- Software Utilities
- Safe Software Storage
- Backup Controls

Privileged Entity Controls / Privileged operations functions:

- Special access to system commands
- Access to special parameters
- Access to the system control program

Media Resource Protection:

Are implemented to protect any security threat by intentional or unintentional exposure of sensitive data -

- Media Security Controls:

Should be designed to prevent the loss of sensitive information and can be:

- Logging
- Access control
- Proper disposal
- Media Viability Controls

Should be used to protect the viability of the data storage media.

Is required in the event of system recovery process -

- Marking
- Handling
- Storage

Physical Access Controls:

Covers

- Hardware
- Software

Special arrangements for supervision must be made when external support providers are entering a data center.

Piggybacking: Is when an unauthorized person goes through a door behind an authorized person. The concept of a "man trap" is designed to prevent it.

Monitoring and Auditing

Monitoring:

Contains the mechanisms, tools and techniques which permit the identification of security events that could impact the operations of a computer facility.

Monitoring techniques -

- Intrusion detection
- Penetration testing
- Scanning and probing
- Demon Dialling
- Sniffing
- Dumpster Diving
- Social Engineering
- Violation processing using clipping levels

Auditing:

Is the foundation of operational security controls monitoring.

Audit Trails:

Enables a security practitioner to trace a transaction's history.

Problem Management Concepts:

- Reduce failures to a manageable level
- Prevent the occurrence or re-occurrence of a problem
- Mitigate the negative impact of problems on computing services and resources.

Threats and Vulnerabilities

Threats:

Accidental loss:

Is a loss that is incurred unintentionally, though either the lack of operator training or proficiency or by the malfunctioning of an application processing procedure.

- Operator input error and omissions
- Transaction processing errors

Inappropriate Activities:

Is computer behaviour that, while not rising to the level of criminal activity may be grounds for job action or dismissal.

- Inappropriate Content
- Waste of Corporate Resources
- Sexual or Racial Harassment
- Abuse of Privileges or Rights

Illegal Computer Operations and Intentional Attacks:

Computer activities that are considered as intentional and illegal computer activity for personal financial gain for destruction.

- Eavesdropping
- Fraud

- Theft
- Sabotage
- External Attack

Vulnerabilities:

- Traffic / Trend Analysis
- Maintenance Accounts
- Data Scavenging Attacks
- IPL Vulnerabilities
- Network Address Hijacking

E-mail and Internet Security Issues

E-mail:

- SMTP - Works as a message transfer agent.
- POP - Is an Internet mail server protocol that supports incoming and outgoing messages. Once the messages are downloaded from the POP server, they are usually deleted from that server.
- IMAP Is an Internet protocol that enables users to access mail on a mail server. Messages can be downloaded or leave them on the mail server within her remote message folder, referred to as a mailbox.

Hack and Attack Methods:

- Port Scanning and Networking mapping:
Networking mapping tools send out seemingly benign packets to many different systems on a network.
Port scanning identifies open port on a computer.
- Superzapping:
Is a utility used in IBM mainframe centers and has the capability to bypass access control within operating systems.
- Browsing:
Is a general term used by intruder to obtain information that they are not authorized to access. Can be accomplished by looking through another person's files kept on a server or workstation, rummaging through garbage looking for information that was carelessly thrown away or reviewing information that has been saved on diskettes.
- Sniffers
Tools that monitors traffic as it passes by.
The tool is either a piece of hardware or software that runs on a computer with its network interface card (NIC) in promiscuous mode.
- Session Hijacking
An attacker putting herself in the middle of a conversation without being detected.
- Password Cracking
Capture and reveal passwords -
 - Dictionary attack: Is when a large list of words is fed into a hacking tool. This tool runs a one-way hash on the captured password and on each word in the list. The tool compares the hashing results to see if they match. If they do match, the tool has discovered the password, if not it moves to the next word in the list.
 - Brute force attack: A tool will try many different variations of characters, run a hash value on each variation and compare it to the hash value of the captured password.
- Backdoors

Is a program that is installed by an attacker to enable her to come back into the computer at a later date without having to supply login credentials or go through any type of authorization process.

CBK#8 Business Continuity Planning & Disaster Recovery Planning

BCP / Business Continuity Planning

Prime elements:

- Scope and Plan Initiation
- Business Impact Assessment
- Business Continuity Plan Development
- Plan Approval and Implementation

Scope and Plan Initiation:

Marks the beginning of the BCP process

It entails creating the scope for the plan.

Roles and Responsibilities -

The BCP Committee:

Should be formed and given the responsibility to create, implement and test the plan.

Is made up of representatives from senior management, all functional business units, information systems and security administrator.

Senior Management's Role:

Is ultimate responsible for all four phases of the plan.

BIA / Business Impact Assessment:

Is a process used to help business units understand the impact of a disruptive event.

The impact may be financial (quantitative) or operational (qualitative, such as the inability to respond to customer)

A vulnerability assessment is often a part of the BIA process.

It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of a disaster or disruption.

Three main primary goals of BIA -

- Criticality Prioritization:

Every critical business unit process must be identified and prioritized and the impact of a disruptive event must be evaluated.

- Downtime Estimation:

Estimates the MTB / Maximum Tolerable Downtime that the business can tolerate and still remain a viable company.

- Resource Requirements:

The resource requirements for the critical processes are also identified at this time, with the most time-sensitive processes receiving the most resource allocation.

Four steps of BIA -

- Gathering the needed assessment materials:

Identifying which business units is critical to continuing an acceptable level of operations.

- Performing the vulnerability assessment:

Is smaller than a full risk assessment and is focused on providing information that is used solely for the BCP or DRP.

A function is to conduct a loss impact analysis.

Critical support areas must be defined.

- Analyzing the information compiled:

Business Continuity Plan Development:

Refers to using the information collected in the BIA to develop the actual business continuity plan.

This includes the areas of plan implementation, plan testing and ongoing plan maintenance.

Two main steps -

- Defining the continuity strategy:

How the business is supposed to manage a disaster disruption.

- Documenting the continuity strategy:

Creation of documentation for the results.

Plan Approval and Implementation:

Involves getting the final senior management sign-off, creating enterprise-wide awareness of the plan and implementing a maintenance procedure for updating the plan as needed.

DRP / Disaster Recovery Planning

Is a comprehensive statement of consistent actions to be taken before, during and after a disruptive event that causes a significant loss of information systems resources.

The primary objective is to provide the capability to implement critical processes at an alternate site and return to the primary site and normal processing within a time frame that minimizes the loss to the organization, by executing rapid recovery procedures.

Disaster planning process phases:

- Data Processing Continuity Planning
- Data Recovery Plan Maintenance

Data Processing Continuity Planning:

Common alternative processing types -

- Mutual aid agreements / Reciprocal agreements:

Is an arrangement with another company that may have similar computing needs.

Advantages is low cost

Disadvantages is that it is highly unlikely that each organization's infrastructure will have the extra capacity to enable full operational processing during the event.

- Subscription services:
 - Hot site:

Is a fully configured computer facility with electrical power, heating, ventilation and air conditioning (HVAC) and functioning file/printer servers and workstations.

Advantage is a 24/7 availability.

Disadvantage is that it is expensive, the service provider might oversell capacity, security exposure when information is stored in two places and may be administrative resource intensive when controls must be implemented twice.

- Warm site

Is a facility readily available with electrical power and HVAC and computers, but the applications may not be installed.

Advantages is that costs is less than a hot site, more flexible in the choice of site(location) and less administrative resources than a hot site.

Disadvantage is the difference in amount of time and effort it will take to start production processing at the new site.

- Cold site

Is ready for equipment to be brought in during emergency, but no hardware resides at the site.

Advantages is low cost.

Disadvantage is that it may not work when a disaster strikes.

- Multiple centers:

The processing is spread over operations centers, creating a distributed approach to redundancy and sharing of available resources.

Advantage is low cost.

Disadvantage is that a major disaster could easily overtake the processing capability of the sites.

- Service bureaus:

Contract with a service bureau to provide all alternate backup processing services.

Advantage is quick response and availability

Disadvantage is the expense and resource contention during a large emergency.

- Other data center backup alternatives:

- Rolling/mobile backup sites

- In-house or external supply of hardware replacements

- Prefabricated buildings

Three concepts used to create a level of fault tolerance and redundancy in transition processing:

- Electronic vaulting:

Refers to the transfer of backup data to an off-site location. This is primarily a batch process of dumping the data through communications lines to a server at an alternative location.

- Remote journaling:

Refers to the parallel processing of transactions to an alternate site. A communication line is used to transmit live data as it occurs.

- Database shadowing:

Uses the live processing of remote journaling but creates even more redundancy by duplicating the database sets to multiple servers.

Data Recovery Plan Maintenance:

Keeping the plans up-to-date and relevant.

Testing the DRP / Disaster Recovery Plan:

Types of test types -

- Checklist:

Copies of plan are distributed to management for review.

- Structured Walk-Through:

Business unit management meets to review the plan.

- Simulation Test:

All support personnel meet in a practice execution session.

- Parallel Test:

Critical systems are run at an alternate site.

- Full-Interruption Test:

Normal production shut down, with real disaster recovery processes.

Primary elements of the disaster recovery process -

- The recovery team:

Will be clearly defined with the mandate to implement the recovery procedures at the declaration of the disaster.

The primary task is to get the pre-defined critical business functions operating at the alternate backup processing site.

- The salvage team:

Will be dispatched to return the primary site to normal processing environmental conditions.

This team is often given the authority to declare when the site is resumptive or not.

- Normal operations resume:

Full procedures on how the company will return production processing from the alternate site to the primary site with the minimum of disruption and risk.

The emergency is not over until all operations are back in full production mode at the primary site.

- Other recovery issues:

- Interfacing with external groups

- Employee relations

- Fraud and crime

- Financial disbursement

- Media relations

CBK#9 Law, Investigations & Ethics

Ethics

ISC2:

Code of Ethics Canons -

- Protect society, the commonwealth and the infrastructure
- Act honorably, honestly, justly, responsibly and legally
- Provide diligent and competent service to principals.
- Advance and protect the profession.

IAB - Internet Activities Board:

Unethical and unacceptable behaviour –

- Purposely seeking to gain unauthorized access to Internet resources
- Disrupting the intended use of the Internet.
- Wasting resources through purposeful actions
- Destroying the integrity of computer-based information.
- Compromising the privacy of others.
- Involving negligence in the conduct of Internet-wide experiments

GASSP - Generally Accepted System Security Principles:

Seeks to develop and maintain GASSP with guidance from security professionals, IT product developers, information owners and other organizations having extensive experience in defining and stating the principles of information security.

MOM - Motivations, Opportunities and Means:

Motivations – Who and why of a crime

Opportunities - Where and when of a crime

Means - The capabilities a criminal would need to be successful.

Operations security

Salami:

Involving subtracting a small amount of funds from an account with the hope that such an insignificant amount would be unnoticed

Data Diddling:

Refers to the alteration of existing data and many times this modification happens before it is entered into an application or as soon as it completes processing and is outputted from an application

Excessive Privileges:

Occurs when a user has more computer rights, permissions and privileges than what is required for the tasks she needs to fulfill.

Password Sniffing:

Sniffing network traffic in the hopes of capturing passwords being sent between computers.

IP Spoofing:

Manually change the IP address within a packet to point to another address.

Denial of Service - DoS:

Denying others the service that the victim system usually provides.

Dumpster Diving:

Refers to someone rummaging through another person's garbage for discarded document, information and other precious items that could then be used against that person or company.

Emanations Capturing:

Eavesdropping of the electrical waves emitted by every electrical device.

Wiretapping:

Eavesdropping of communication signals.

Social Engineering:

The art of tricking people and using the information they know unknowingly supply in a malicious way.

Masquerading:

A method that an attacker can use to fool others of her real identity

Liability and Its Ramifications

Due Care:

Steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and have taken the necessary steps to help protect the company, its resources and employees.

Due Diligence:

Continual activities that make sure the protection mechanisms are continually maintained and operational.

Prudent man rule:

To perform duties that prudent people would exercise in similar circumstances.

Downstream liabilities:

When companies come together to work in an integrated manner, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability and responsibility needed which should be clearly defined in the contracts that each party signs.

Legally recognized obligation:

There is a stand of conduct expected of the company to protect others from unreasonable risks. The company must fail to conform to this standard, which results in injury or damage to another.

Proximate causation:

Someone can prove that the damage that was caused was the company's fault.

Types of Laws

Civil law:

Also called Tort.

Deals with wrongs against individuals or companies that result in damages or loss

A civil lawsuit would result in financial restitution instead of jail sentences.

Criminal law:

Is used when an individual's conduct violates the government's laws, which have been developed to protect the public.

Jail sentences are commonly the punishment.

Administrative law:

Deals with regulatory standards that regulate performance and conduct.

Government agencies create these standards, which are usually applied to companies and individuals, within those companies.

Intellectual Property Laws

Trade secret:

The resource that is claimed to be a trade secret must be confidential and protected with certain security precautions and actions.

Copyright:

Protects the expression of the idea of the resource.

Trademark:

Is used to protect a word, name, symbol, sound, shape, colour, device or combination of these.

Patent:

Are given to individuals or companies to grant the owner legal ownership and enable the owner to exclude others from using and copying the innovation covered by the patent. A patent grants a limited property right for 17 years.

Computer Crime Investigations

Incident response team:

Basic items -

- List of outside agencies and resources to contact or report to.
- List of computer of forensics experts to contact.
- Steps on how to secure and preserve evidence.
- Steps on how to search for evidence
- List of items that should be included on the report.
- A list that indicates how the different systems should be treated in this type of situation.

Computer Forensics:

Forensics investigation -

1st step: Make a sound image of the attacked system and perform forensic analysis on this copy. This will ensure that the evidence stays unharmed on the original system in case some steps in the investigation actually corrupt or destroy data. Also the memory of the system should be dumped to a file before doing any work on the system or powering it down.

2nd step / Chain of custody: Must follow a very strict and organized procedure when collecting and tagging evidence.

Dictates that all evidence be labeled with information indication who secured and validated it. The chain of custody is a history that shows how evidence was collected, analyzed, transported and preserved in order to be presented as evidence in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

The life cycle of evidence:

Includes following

- Collection and identification
- Storage, preservation and transportation.
- Presentation in court
- Being returned to victim or owner.

Evidence:

Best evidence - Is the primary evidence used in a trial because it provides the most reliability. Is used for documentary evidence such as contracts.

Secondary evidence - Is not viewed as reliable and strong in proving innocence or guilt when compared to best evidence.

Direct evidence - Can prove fact all by itself instead of needing backup information to refer to.

Conclusive evidence - Is irrefutable and cannot be contradicted.

Circumstantial evidence - Can prove an intermediate fact that can then be used to deduce or assume the existence of another fact.

Corroborative evidence - Is supporting evidence used to help prove an idea or point. It cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence.

Opinion evidence - When a witness testifies, the opinion rule dictates that she must testify to only the facts of the issue and not her opinion of the facts.

Hearsay evidence - Pertains to oral or written evidence that is presented in court that is secondhand and that has no firsthand proof of accuracy or reliability.

Characteristics of evidence:

Must be

Sufficient - It must be persuasive enough to convince a reasonable person of the validity of the findings. Means also that it cannot be easily doubted.

Reliable / Competent - It must be consistent with fact, must be factual and not circumstantial.

Relevant - It must have a reasonable and sensible relationship to the findings.

Legally permissible - It was obtained in a legal way.

Enticement <-> Entrapment:

Enticement -

Is legal and ethical.

Entrapment -

Is neither legal nor ethical.

Phone Phreakers

Blue boxing - A device that simulates a tone that tricks the telephone company's system into thinking the user is authorized for long distance service, which enables him to make the call.

Red boxes - Simulates the sound of coins being dropped into a payphone.

Black boxes - Manipulates the line voltage to receive a toll-free call.

CBK#10 Physical Security

Physical Security Controls

Types of controls:

- Administrative controls
 - Facility selection or construction
 - Facility management
 - Personnel controls
 - Training
 - Emergency response and procedures
- Technical controls
 - Access controls
 - Intrusion detection
 - Alarms
 - Monitoring (CCTV)
 - Heating, ventilation and air conditioning (HVAC)
 - Power supply
 - Fire detection and suppression
 - Backups
- Physical controls
 - Fencing
 - Locks
 - Lighting
 - Facility construction materials

Facility Management

Issues with selecting a location:

- Visibility
- Surrounding area and external entities
- Accessibility
- Natural disaster

Construction issues when designing and building a facility:

- Walls
- Doors
- Ceilings
- Windows
- Flooring
- Heating and Air Conditioning
- Power Supplies
- Water and Gas Lines
- Fire Detection and Suppression

Concerns:

The load - How much weight that can be held of a building's walls, floors and ceilings needs to be estimated and projected to ensure that the building will not collapse in different situations.

Positive flow (water and gas lines) - Material should flow out of building, not in.

Internal partitions - Many buildings have hung ceilings, meaning the interior partitions may not extend above the ceiling; therefore an intruder can lift a ceiling panel and climb over the partition.

Physical Security Component Selection Process

Security Musts:

Obligated by law to obey certain safety requirements

Security Shoulds:

Protection procedures that should be put into place to help protect the company from devastating activities and their results.

Hardware:

SLAs / Servicelevel agreements - Ensure that vendors provide the necessary level of protection.

MTBF / Mean Time Between Failure - Is used to determine the expected lifetime of a device or when an element within that device is expected to give out.

MTTR / Mean Time To Repair - Is used to estimate the amount of time between repairs.

Power Supply:

Power protection -

- Online systems: Use a bank of batteries
- Standby UPS: Stay inactive until a power line fails
- Backup power supplies: Used to supply main power or charge batteries in a UPS system.
- Voltage regulators and line conditioners: Can be used to ensure a clean and smooth distribution of power.

Electrical Power Definitions:

Ground	The pathway to the earth to enable excessive voltage to dissipate
Noise	Electromagnetic or frequency interference that disrupts the power flow and can cause fluctuations
Transient noise	Short duration of power line disruption
Clean power	Power that does not fluctuate
Fault	Momentary power loss/out
Blackout	Complete / Prolonged loss of power
Sag	Momentary low voltage
Brownout	Prolonged low voltage
Spike	Momentary high voltage
Surge	Prolonged high voltage
Inrush	Initial surge of power at the beginning

Environmental issues

Positive drains - Their contents flow out instead of in.

Relative humidity - 40 to 60 % is acceptable

High humidity - Can cause corrosion

Low humidity - Can cause excessive static electricity

Positive pressurization - When an employee opens a door, the air goes out and outside air does not come in.

Fire detectors:

Smoke activated - Photoelectric device.

Heat activated - Rate-of-rise temperature sensors and fixed-temperature sensors.

Flame activated - Senses the infrared energy

Automatic Dial-up Alarm - Call the local fire station to report detected fire.

Fire suppression:

Portable extinguishers should be located within 50 feet of any electrical equipment and located near exits.

Fire classes and suppression medium:

A	Common combustibles	Water or Soda Acid
B	Liquid	CO2, Soda Acid or Halon
C	Electrical	CO2 or Halon

Water - Suppresses the temperature required to sustain the fire.

Soda Acid - Suppresses the fuel supply of the fire

CO2 - Suppresses the oxygen supply required to sustain the fire

Halon - Suppresses the combustion through a chemical reaction

Replacement list for Halon:

FM-200, NAF-S-III, CEA-410, FE-13, Water, Inergen, Argon, Argonite.

Water Sprinkler:

Wet Pipe - Always contain water in the pipes and are usually discharged by temperature control level sensors.

Dry Pipe - The water is held by a valve until a specific temperature is reached. There is a time delay between the predefined temperature being met and the release of water.

Preaction - Combine the use of wet and dry pipe system. Water is not held in the pipes and is only released into the pipes once a predefined temperature is met. Once this temperature is met, the pipes are filled with water, but it does not release right away. A link has to melt before the water is released from the sprinkler head itself.

Deluge - The same as a dry pipe system except the sprinkler head is open.

Perimeter Security

Facility Access Control:

Enforced through physical and technical components

Locks:

Are the most inexpensive access control mechanisms.

Are considered deterrent to semiserious intruders and delaying to serious intruders.

Preset Locks - Are locks usually used on doors.

Cipher Locks / programmable locks - Use keypads to control access into an area or facility.

Options available on many cipher locks:

- Door delay: If the door is held open for a long period of time, an alarm will trigger to alert personnel of suspicious activity.
- Key-override: A specific combination can be programmed to be used in emergency situations to override usual procedures or for supervisory overrides.
- Master-keying: Enables supervisory personnel to change access

codes and other features of the cipher lock.

- Hostage alarm: If an individual is in duress and/or held hostage, there can be a combination he or she enter to communicate this situation to the guard station and/or police station.

Device Locks - To protect devices by using Switch controls, slot locks, port controls, peripheral switch control and cable traps.

Personnel Access Controls:

Proper identification to verify if the person attempting to access a facility or area should actually be allowed in.

Piggybacking - When an individual gains unauthorized access by using someone else's legitimate credentials or access rights.

Magnetic cards:

Memory card - The reader will pull information from it and make an access decision.

Smart card - The individual may be required to enter a PIN or password, which the reader compares against the information held within the card.

Wireless Proximity Readers:

User activated - Transmits a sequence of values to the reader

System sensing - Will recognize the presence of the coded device within a specific area.

- Transponders: The card and reader have a receiver, transmitter and battery
- Passive devices: The card does not have any power source of its own
- Field-powered devices: The card and reader contain a transmitter and active electronics.

External Boundary Protection Mechanism:

Fencing:

3-4 feet - Deter casual trespassers

6-7 feet - Considered too high to climb easily

8 feet with 3 strands of barbed wire - Deter intruders

Mantrap - The entrance is routed through a set of double doors that may be monitored by a guard.

Lighting:

Should be used to discourage intruders and provide safety for personnel, entrances, parking areas and critical sections.

Critical areas should be illuminated 8 feet high and 2 feet out.

Surveillance Devices:

Three main categories -

- Patrol Force and Guards - Can make determinations
- Dogs - Are loyal, reliable and have a sense of smell and hearing
- Visual Recording Devices: Camera, CCTV, ...

Detecting:

Proximity Detection System / Capacitance detector -

Emits a measurable magnetic field while in use. The detector monitor this electrical field and an alarm sounds if the field is disrupted.

Photoelectric or Photometric System -

Detects the change in the level of light within an area.

Wave Patterns -

Generates a wave pattern that is sent over an area and reflected back to the receiver.

Passive Infrared System -

Identifies the changes of heat waves with an area it is configured to protect.

Acoustical-Seismic Detection System -

Is sensitive to sounds and vibrations and detects the changes in the noise level of an area it is placed.

Media Storage Requirements

Data that is no longer needed or used must be destroyed.

Object reuse - The concept of reusing data storage media after its initial use

Data remanence - Is the problem of residual information remaining on the media after erasure.

Stages of data erasure -

- Clearing: Overwriting of data/media intended to be reused in the same organization or monitored environment.

- Purging: Degaussing or overwriting media intended to be removed from a monitored environment.

- Destruction: Completely destroying the media and therefore residual data.

Related links

On the Internet you can find many sites covering information security. All of them are not a relevant study guide for IS professionals, but may include very interesting information. The links listed below are just some of all those links.



(ISC)2

www.isc2.org

The starting point for your CISSP examination



CCCURE

www.cccure.org

The best studyguide for the CISSP examination, with documents and links.



ISACA

www.isaca.org

Foundation for information security auditors, administers the CISA certification.



CERT Coordination Center

www.cert.org

A center of Internet security expertise.



Incidents.org

www.incidents.org

A virtual organization of advanced intrusion detection analysts, forensics experts and incident handlers.



NIST CSRC

www.csrc.nist.gov

Computer Security Resource Center at NIST .

References

When preparing for the CISSP exam, there are a lot of books and references you may use. For my preparation the references listed below have been used.



CISSP all-in-one Certification Exam Guide

Shon Harris

Has been the primary study guide for me. Practice questions are included in the book and on a CD.



The CISSP Prep Guide

Ronald L. Krutz and Russel Dean Vines

Was a supplementary study guide for me. Practice questions are included in the book.



ISO/IEC 17799

ISO standard (prior the british standard BS 7799)

Code of practice for information security. The basis for ISO certification in Information Security.



CCCURE

www.cccure.org

Already mentioned. Still you will find reference material for your preparation here..