INFORMATION SECURITY NOTES

FINAL

Michael R. Overly, Esq., CISSP

moverly@foleylaw.com

Modified by Jane E. Murley, CISSP, MCSE, GSEC

murley@starpower.net

I. **CBK #1: Operations Security**

    A. **Types:**

        1. **Preventive** — Designed to lower amount and impact of unintentional errors entering the system and to prevent unauthorized intruders from internally or externally accessing the system — actions to reduce risk
Data validation, pre-numbered forms, and review for duplications

        2. **Detective** — Identify and react to security violations
Track unauthorized transactions and lessen errors by detecting quickly.

        3. **Corrective** — React to an attack and take corrective action
Data recovery

        4. **Recovery** — Restore the operating state to normal after an attack or system failure

    B. Orange Book — Trusted Computer Security Evaluation Criteria — Two types of assurance:

        1. **Operational Assurance** — (1) System architecture, (2) system integrity, (3) covert channel analysis (4) trusted facility management, (5) trusted recovery

            a. **Trusted facility management**: assignment of specific individual to administer security of system — Separation of duties, don't have system administrator and security administrator as same person — In highly secure systems have three administrative roles: system administrator, security administrator, and enhanced operator function — Two-man control means each reviews and approves the work of the other — Dual control requires both operators to complete a task — Rotation of duties — Mandatory one week vacations

            b. **Trusted recovery**: ensures security is not breached when system crashes or has other failures — Required only for B3 and A1 levels in Orange Book

       c.   Common Criteria for recovery:

          (i)   Manual Recovery — System administrator intervention to return system to secure state after failure

          (ii)   Automated Recovery —— Recovery to secure state is automatic when resolving <u>single</u> failure – intervention for other failures.

          (iii)   Automated Recovery without Undue Loss —

   2.   **Live cycle assurance** — Controls needed for building and maintaining system — Configuration management monitors and protects changes to a system's resources — Security testing
(1) security testing, (2) design specification and testing, (3) configuration management, (4) trusted distribution

       a.   Configuration change management (<u>covers entire lifecycle of system/software</u>) — Required only for B2, B3, and A1 — Five procedures:

          (i)   Applying to introduce a change

          (ii)   Cataloging the change

          (iii)   Scheduling the change

          (iv)   Implementing the change

          (v)   Reporting the change to appropriate parties

       b.   Trusted distribution — procedures to ensure that all of the TCB configuration items, such as the TCB software, firmware, hardware, and updates, distributed to a customer site arrive exactly as intended by the vendor without any alterations

C.   Media security controls — Logging, access control, and proper disposal —— Sanitization includes overwriting, degaussing, and destruction — Media viability controls: marking, handling, storage

D.   Problem management goals:

   1.   Reduce failures to a manageable level

   2.   Prevent occurrence or re-occurrence of a problem

   3.   Mitigate negative impact of problems

E.   Initial Program Load (IPL) vulnerabilities

F.   Three general reboot categories after failure or crash

   1.   System reboot

2. System cold start

3. Emergency system restart

G. Security Issues

1. Fail Secure (CC)

2. Software Piracy

3. Media disposal

4. Dumpster diving

5. Data Remanence — residual data remaining on media after erasure

6. Fraud — countermeasures: job rotation, separation of duties, mandatory vacation

II. **CBK #2: Security Architecture and Models**

A. OS components: process management, I/O, memory management, and system file management

B. Multiprocessing – means multiple processors

C. IT Architecture: logical (functional) and technical (physical) components

D. Closed security environment: (i) application developers have sufficient clearances and authorizations to provide acceptable presumption that they will not introduce malicious logic and (ii) configuration control provides protection from introduction of malicious logic prior to and during the operation of systems — Open security environment does not have the foregoing protections

E. Types of I/O: Block devices (write blocks of data; hard disk) and character devices (not addressable; keyboard and printer)

F. CPU operating states: ready state, problem state, supervisory state, and wait state

G. Programming languages — Three types: machine (1GL), assembly (2GL), and high-level (3-5GL)

1. Assembler – translates from assembly language to machine language.

2. Disassembler – translates machine language to assembly.

3. Compiler – translates high-level language to machine code.

4. Decompiler – translates machine language into high-level language.

5. Interpreter – translates high-level language one command at time to machine code.

H. Staffing: define position, determine sensitivity of position, filling position, training hired person.

I. Delphi Technique — Group does not meet as a whole — Individual members submit anonymous comments.

J. Causes of economic loss: 65% errors and omissions.

K. Total Quality Management (TQM): (1) pursuit of complete customer satisfaction, (2) continuously improve products and services, through (3) the full and active involvement of the entire workforce
Quality Assurance typically focuses on the quality of the end-product
Under TQM, QA focuses on assuring quality throughout production and service process
Quality Circles are team of voluntary employees that get together to discuss quality issues
Quality Council is management

L. ISO 9000: addresses quality of system processes not product performance to specifications — Provides baseline for TQM

M. Benchmarking:

  1. Internal

  2. Competitive

  3. Industry

  4. Best-in-Class

N. Dynamic RAM (DRAM; multi-phase clock signals) and SRAM (single-phase clock)– refresh.

O. Programmable Logic Device (PLD): IC with connections or internal logic gates that can be programmed

P. Memory: Real or Primary (RAM), Secondary (hard disk), Sequential Memory – information must be obtained sequentially searching from the beginning (tape).

Q. CPU States

  1. Problem state — executing an application

  2. Wait state — waiting for a specific event to complete

  3. Ready state — an application is ready to resume processing

  4. Supervisory state — executing in privilege mode

R. Pipelining: overlaps steps of instructions

S. Scalar processor – executes one instruction at a time

T. Multiprogramming, multitasking, multiprocessing

U. I/O: memory mapped and isolated — Collectively "Programmed I/O"

V. Protection Domain: execution and memory space assigned to each process

W. Trusted computer base (TCB): total combination of protection mechanisms within a system —— Security perimeter is boundary separating TCB from remainder of system —— TCB must be tamperproof and non-compromisable

X.   **Security Kernel** is hardware, software, firmware, elements of TCB that implement the reference monitor concept — must be isolated from reference monitor

Y.   **Reference monitor** is a system component that enforces access controls on an object — Reference monitor concept is an abstract machine that mediates all access of subject to objects — Must be verified correct

Z.   Security Modes of Operation:

1.   **Dedicated Security Mode**: Each subject must have clearance for <u>all</u> information on system and valid need to know for <u>all</u> information.

2.   **System high Security Mode**: Each subject must have clearance for <u>all</u> information on system and valid need to know <u>some</u> of the information ——All users may not have need to know ——

3.   **Compartmented Security Mode**: Each subject must have clearance for <u>most restricted</u> information on system and valid need to know <u>that</u> information.

4.   **Multilevel Mode**: Some subjects do not have clearance for <u>all</u> information — — Each subject has a need to know <u>all</u> information to which they will have access.

AA.   Recovery procedures: system should restart in secure mode

1.   Startup should occur in maintenance mode that permits access only by privileged users from privileged terminals

2.   Fault-tolerant continues to function despite failure

3.   Fail safe system, program execution is terminated and system protected from compromise when hardware or software failure occurs

4.   Fail soft or resilient system, selected, non-critical processing is terminated when failure occurs

5.   Failover, switches to hot backup.

BB.   Assurance – degree of confidence in satisfaction of security requirements

1.   Evaluation criteria:

a.   Trusted Computer Security Evaluation Criteria (TCSEC): addresses confidentiality, not integrity — Focuses on security <u>functionality</u> and degree of <u>assurance</u> that functionality works as documented — Functionality and assurance requirements are combined in TCSEC ratings

Five aspects of security:

(i)   System security policy,

(ii)   Marking (use of labels for AC),

(iii)   Identification of individuals,

5

(iv)   Accountability mechanisms on the system, operational and lifecycle assurance of system's security

(v)   Documentation developed and maintained about system security

Limited to the OS — Orange book

D — Minimal Protection – system tested and failed

C — Discretionary Protection (C1 and C2)

B — Mandatory Protection (B1, B2, and B3)

    B1 labels for AC

    B2 addresses covert channels and includes trusted facility management; configuration management

    B3 TCB design directed to minimizing complexity; use of security administrator and auditing; configuration management.

A — Verified protection (A1) — A1 configuration management

b.   Trusted Network Interpretation (TNI): addresses confidentiality and integrity — Red book

c.   European Information Technology Security Evaluation Criteria (ITSEC)

Addresses confidentiality, integrity, and availability — Focuses on functionality and assurance

Two levels for each system: "F" for functionality (F1 – F10) and "E" for European Assurance (E0 – E6; E6 is highest) — F1 is comparable to C1 of Orange Book

Target of Evaluation (TOE) is product or system to be evaluated

Functionality and assurance are evaluated independently under ITSEC — Compare TCSEC, which combines functionality and assurances into a single set of classes

d.   TCSEC, ITSEC, and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) have evolved into one evaluation criteria: <u>Common Criteria</u>

CC.   Certification: Establish extent in which a particular design and implementation meets the set of specified security requirements.

DD. Accreditation: Formal declaration by Designated Approving Authority that system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

    1. Defense Information Technology Security Certification and Accreditation Process (DITSCAP): Phase 1 definition, phase 2 verification, phase 3 validation, phase 4 post accreditation.

    2. National Assurance Certification and Accreditation Process (NIACAP)

EE. Information Security Models: Access control, integrity, and information flow

    1. Access Control Model — Four methods:

        a. Access Matrix – Columns are ACLs and rows are capability lists — Includes DAC — Capability list: used to implement capabilities, which identifies the object and specifies the access rights to be allowed to the subject who possesses the capability.

        b. Take-Grant Model

        c. Bell-La Padula Model — Only addresses confidentiality, not integrity or availability — A Trusted Subject can violate the *property — Does not address client/server model — Secure state can have three properties:

            (i) Simple Security Property (ss Property): reading info by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up);

            (ii) The * star Security Property: writing info by subject at higher level of sensitivity to an object at lower sensitivity is not permitted (no write down).

            (iii) Discretionary Security Property — Uses an access matrix to specify DAC

    2. Integrity Model

        a. Biba Integrity Model (similar to Bell-La Padula)

        b. Clark-Wilson Integrity Model — Two elements: well formed transaction and separation of duties.

    3. Information Flow Model – each object and subject is assigned security class and value; info is constrained to flow in directions that are permitted by the security policy.

III. **CBK #3: Business Continuity Planning and Disaster Recovery Planning.**

A. Business Continuity Planning (BCP) — Plans and framework to ensure business can continue in an emergency — Minimize cost associated with disruptive event and mitigate risk — Foreign Corrupt Practices Act of 1977 imposes civil and criminal penalties if publicly held companies fail to maintain adequate controls over their info systems

Four elements of BCP process:

1. Scope and Plan Initiation

   a. Creating a detailed account of the work required

   b. Listing the resources to be used

   c. Defining the management practices to be employed

   d. Defining goals — established to keep everyone on track and ensure that the efforts pay off in the end

2. Business Impact Assessment (BIA)

   a. Identify what impact a disruptive event would have on the business — Impact may be financial (quantitative) or operational (qualitative)

   b. BIA has three goals: criticality prioritization, maximum tolerable downtime estimation, resource requirements

   c. Must identify which business units are critical to continuing acceptable level of operations

   d. Steps include:

      (i) Gather the needed assessment materials

      (ii) Performing the vulnerability assessment — involves conducting a loss impact analysis — Two elements: financial assessment (quantitative) and operational assessment (qualitative) — Identify "critical support areas" that are required to sustain continuity of business

      (iii) Analyzing the information compiled

      (iv) Documenting the results and presenting recommendations

3. Business Continuity Plan Development

   a. Document all costs with alternatives

   b. Address five categories: business recovery, facility and supply, user, technical/operational, and data

  4. Plan Approval and Implementation

   a. Senior management must approve plan

   b. Test plan

   c. Regularly review plan and update

B. Disaster Recovery Planning (DRP) —

  1. Quickly recovering from an emergency with minimum of impact on business

  2. Plan of action for before, during, and after a disruptive event

  3. Primary objective: capability to move critical processes to an alternate site and return to the primary site and normal processing within a time frame that minimizing loss to the organization — Number one priority is people

  4. **Plan from top down**

  5. Two steps in DRP planning process:

   a. Data processing continuity planning

    (i) Mutual aid agreements — An arrangement with another company that may have similar computing needs, similar hardware or software configurations and may require the same network data communications

    (ii) Subscription services:

     a) Hot site — a fully configured computer facility with electrical power, heating, ventilation, and air conditioning (HVAC) and functioning file/print servers and workstations

     b) Warm site — computer facility available with electrical power, heating, ventilation, and air conditioning (HVAC), limited file/print servers and workstations

     c) Cold site — computer facility available with electrical power, heating, ventilation, and air conditioning (HVAC) – no computer hardware

    (iii) Multiple centers — Processing is spread over several operations centers, creating a distributed approach to redundancy and sharing of available resources

    (iv) Service bureaus — Use service bureau to fully provide all alternate backup processing services

<div align="center">9</div>

(v) Other data center alternatives — For example transaction redundancy implementations:

  d) Electronic Vaulting – transfer of backup data to an offsite location — Done batch over telecom lines to alternate location

  e) Remote Journaling – parallel processing of transactions to an alternate site — Telecom line transmits live data as it occurs

  f) Database Shadowing – uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers

 b. Data recovery plan maintenance — Keeping plan up to date

C. Disaster Recovery Plan Testing – five types of testing (don't disrupt normal business functions) — Testing is used to find weaknesses in plan:

 1. Checklist – copies of plan are distributed for management to review.

 2. Structure walk through – business unit management meets to review plan

 3. Simulation – Support personnel meet in a practice execution session — no actual recovery process performed

 4. Parallel – critical systems run at an alternate site — results compared with actual production results

 5. Full-Interruption – normal production shut down, with real disaster recovery processes.

D. Recovery process:

 1. Recovery team — Get pre-defined critical business functions operating at the alternate backup processing site

 2. Salvage Team — Return the primary site to normal processing environmental conditions

 3. Normal operations resume – least critical work done first

 4. Other recovery issues

E. Contingency Planning — Provides alternatives for those chance events that could impact normal operations — Two essentials for contingency planning: information backup and management commitment — Includes three parts: emergency response, recovery, and resumption

F. Hierarchical Storage Management (HSM) — Software that dynamically manages storage and retrieval of electronic information from storage media that varies in speed and cost

G. Six resource categories that support critical business functions: human resources, processing capability, computer-based services, automated applications and data, physical infrastructure, and documents

IV. **CBK #4: Security Management Practices**

A. <u>Primary Concepts</u>: CIA (opposite is DAD – destruction, alteration, and disclosure)

    1. **Confidentiality** — information classification

    2. **Integrity:** Three principles to establish integrity controls: (i) granting access on need-to-know basis; (ii) separation of duties; and (iii) rotation of duties — Firewalls, IDS — Types of integrity:

        a. Modifications made by unauthorized personnel or processes

        b. Unauthorized modifications by authorized personnel or processes

        c. Internal and external consistency

    3. **Availability –** fault tolerance, backups

B. <u>Secondary Concepts</u>

    1. **Identification** – means by which users identify themselves to the system

    2. **Authentication** – testing or reconciliation of evidence of user's identity

    3. **Accountability** – System ability to determine actions of user within the system and to identify the user — Audit trails (must be protected) and log files.

    4. **Authorization** – rights and permissions granted to a user or process — ACL

    5. **Privacy** – Level of confidentiality and privacy protection of a user

C. Audit trails: user accountability; reconstruction of events, intrusion detection, and problem analysis — Audit records: keystroke monitoring/logging and event-oriented logs — Protect integrity by requiring digital signatures to access, set up as write once — Use software for rapid analysis

D. Security Awareness Training: Awareness (Light: what, recognition, information), training (deeper: how, skill, knowledge), and education (deepest: why, understanding, insight)

E. Most important question to ask in evaluating access control security is to ask how much it is going to cost to not protect the valuable information.

F. **Risk Management (RM)**: Prime objective of security controls is to reduce effects of threats and vulnerabilities to a level that is tolerable (i.e., mitigate risk) — Risk Analysis (RA) — A "risk" is a potential harm or loss to a system; the probability that a threat will materialize

    1. Identifying risks:

        a. Actual threat

b. Possible consequences if threat is realized

c. Probable frequency of occurrence of threat

d. Confidence threat will happen

2. Key Terms

    a. Asset – resource, process, product, system, etc — Value is composed of cost of creation, development, license, support, replacement, public credibility, considered costs, lost IP if disclosed, and ownership values.

    b. Threat – Any event that causes undesirable impact on organization — Data classification, info warfare, personnel, criminal, application, operational

    c. Vulnerability – Absence of safeguard constitutes vulnerability — Risk Management *triple*: Asset, threat, and vulnerability

    d. Safeguard – control or countermeasure to reduce risk associated with a threat

        (i) Absence of safeguard creates a vulnerability

        (ii) Look at cost/benefit analysis of deploying safeguard

        (iii) Include impact on organization of implementing safeguard

        (iv) Safeguard must include ability to audit

        (v) **Value to organization of safeguard** = ALE (before implementation) – ALE (after implementation) – Annualized safeguard cost

        (vi) During or after activation or reset: no asset destruction, no covert channel access to or through control; no security loss or increase in exposure, and defaults to state that does not enable any operator access or rights until controls fully operational

    e. Exposure Factor (EF) – Percentage loss a realized threat would have on an asset — Hardware failure on critical system may result in 100% loss.

    f. Single Loss Expectancy (SLE) – Loss from a single threat

    SLE = Asset Value ($) x EF

g. Annualized Rate of Occurrence (ARO) – estimated frequency in which a threat is expected to occur — Range from 0 (never) to a large number (minor threats, such as misspellings).

h. **Annualized Loss Expectancy (ALE) – ALE = SLE x ARO**

3. Elements of RA

   a. Quantitative RA – Assigns objective dollar cost

   b. Qualitative RA – intangible values of data loss and other issues that are not pure hard costs — results are usually expressed in terms of ordinal ranking

   c. Asset Valuation Process

   d. Safeguard Selection

4. RA Steps

   a. Identify Assets: Estimate potential losses to assets by determining their values

   b. Identify Threats: Analyze potential threats to assets

      if asset has no vulnerabilities, there are no threats and no loss

   c. Calculate risk: Define ALE

5. Remedies: Risk reduction, risk transference (transferring cost of loss to another party (i.e., insurance company)), and Risk acceptance

G. Information Classification

1. Prevent unauthorized disclosure and failure of confidentiality —Demonstrates due diligence, identifies most sensitive info, regulatory compliance, etc — SBU: Sensitive, but unclassified

2. Lattice model: Every resource and user is associated with one of an ordered set of classes — Resources of a particular class may only be accessed by those whose associated class is as high or higher than that of the resource

3. Bell-La Padula Model (Orange Book): most common model

   a. Defines relationships between objects and subjects

   b. Relationships are described in terms of subject's assigned level of access or privilege (security clearance) and the object's level of sensitivity (security classification)

   c. Enforces lattice principle, which specifies that subjects are allowed write access to objects at the same or higher level as the subject, read

13

access to objects at the same or lower level, and read/write access to only those objects at the same level as the subject

        d.   Example of MAC

4.   DOD: unclassified, confidential, secret, top secret

5.   Classification Criteria: Value, Age, Useful Life, and Personally Identifiable.

6.   Procedures:

        a.   Identify administrator/custodian

        b.   Specify classification criteria

        c.   Classify by owner

        d.   Specify exceptions to classification policy

        e.   Specify controls for each classification level

        f.   Specify procedures for declassifying or transferring custody to another entity.

        g.   Enterprise awareness program re classification controls

7.   Roles: Owner (officer or manager), Custodian (day-to-day responsibility for data protection; IT person), and end user (uses info as part of job)

H.   **P**olicies (senior management, regulatory, advisory, informative)

I.   **S**tandards (use of specific technologies in uniform way)

J.   **G**uidelines (recommend actions, but are not compulsory)

K.   **P**rocedures (steps to perform a specific task in compliance with a mandatory standard)

V.   **CBK #5: Access Control Systems**

A.   **Definition**: Set of procedures performed by hardware, software, and administrators, to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules.

B.   ACL: register of (1) users who have been given permission to use an object and (2) the types of access they have been permitted.

C.   **Controls**: Can be used to mitigate risks — Controls can relate to *subjects* (entities or individuals; active entity) or *objects* (files, systems, or other resources; passive entities) — Controls can be *preventive*, *detective*, or *corrective* — These can be implemented by:

14

1. <u>Administrative controls</u>: policies and procedures, disaster recovery plans, awareness training, security reviews and audits, background checks, review of vacation history, separation of duties, and job rotation.

2. <u>Logical or technical controls</u>: Restrict access to systems and the protection of information — Encryption, smart cards, anti-virus software, audit trails, log files, ACLs, biometrics, and transmission protocols (Kerberos, IPSec) —

3. <u>Physical controls</u>: guards and building security, biometric access restrictions, protection of cables, file backups

D. **Constrained User Interface** – menus and shells; database views; and physically constrained user interfaces (limited number of buttons – ATM machine)

E. **Three types of access rules**:

1. <u>Mandatory access control (MAC)</u>: Authorization of subject's access to an object depends on labels (sensitivity levels), which indicate subject's clearance, and the classification or sensitivity of the object

   a. Every Object is assigned a sensitivity level/label and only users authorized up to that particular level can access the object

   b. Access depends on rules and not by the identity of the subjects or objects alone

   c. Only administrator (not owners) may change category of a resource — Orange book B-level

   d. Output is labeled as to sensitivity level

   e. Unlike permission bits or ACLs, labels cannot ordinarily be changed

   f. Can't copy a labeled file into another file with a different label

   g. <u>Rule based</u> AC

2. <u>Discretionary Access Control (DAC)</u>: Subject has authority, within certain limits, to specify what objects can be accessible (e.g., use of ACL)

   a. User-directed means a user has discretion

   b. Identity-based means discretionary access control is based on the subjects identity

   c. Very common in commercial context because of flexibility

   d. Orange book C level

   e. Relies on object owner to control access

   f. <u>Identity Based</u> AC

15

3. <u>Non-Discretionary Access Control</u>: Central authority determines what subjects can have access to certain objects based on organization's security policy

    a. May be based on individual's role in the organization (<u>Role-Based</u>) or the subject's responsibilities or duties (task-based)

F. **Checksum** — Have checksum of program files to see if they have been altered — Only should change when updates are installed — Use to find changes made by Superzap

G. **Intrusion Detection Systems (IDS)**:

1. Monitors network traffic or to monitor host audit logs to detect violations of security policy — Detects attacks by two major mechanisms: signature – based ID (knowledge-based) or a statistical anomaly-based ID (Behavior-based)

2. Two general types:

    a. <u>Network-Based IDS</u>: Doesn't consume network or host resources — Reviews packets and headers — Monitors network traffic in real time — Won't detect attacks against a host by a user logged in at the host's terminal (only the network is monitored)

    b. <u>Host-Based IDS</u>: Reviews system and event logs to detect attack on host — Efficacy is limited by lack of completeness of most host audit log capabilities — Resident on centralized hosts

3. Clipping Level: setting thresholds on a reported activity — Clipping level of three can be set for reporting failed workstation logon attempts — Three or fewer won't result in a reported security violation

H. **Authentication**:

1. Identification and authentication are keystones in access control — Establishes an identity, but does not guarantee authorization — Compare authorization, which determines whether a user is permitted to perform some action or access a resource — Authorization and accountability are two separate processes — Three possible factors for authentication:

    a. Something you have (token, key to lock)

    b. Something you know (username and password)

    c. Something you are (biometrics)

2. Methods of authentication: user name and password; x.509 certificate; biometrics; smart cards; anonymous

3. Problems with passwords: can repudiate, insecure, and easily broken

4. Password Management (composition, length, lifetime, source, ownership, distribution, storage, entry, transmission, and authentication period):

16

      a.   Configure system to use string passwords

      b.   Set password time and length limits

      c.   Limit unsuccessful logins

      d.   Limit concurrent connections

      e.   Enable auditing

      f.   Use last login dates in banners

5. Cognitive Passwords — Fact-based cognitive data for user authentication — Favorite color, movie, vegetable

6. **Biometrics**: No common API — Factors: enrollment time (<2 min), throughput rate (6-10 subjects per minute), and acceptability (privacy, invasiveness, can be used to detect health problems, transmission of disease) — Biometric file sizes range from 9-10,000 bytes — Three main performance measurements:

      a.   False Rejection Rate (FRR) or Type I Error: % valid subjects rejected — Too sensitive, too high of a FRR.

      b.   False Acceptance Rate (FAR) or Type II Error: % of invalid subjects falsely accepted — Not sensitive enough, too high of a FAR.

      c.   Crossover Error Rate (CER): % at which FRR=FAR — System with CER of 2% is more accurate than CER of 5%.

7. Two-factor authentication refers to the use of two of the three factors listed above.

8. Static passwords, dynamic passwords (changes with each login), one-time passwords — Pass Phrase – converted by system into a virtual password

9. **Tokens** – Memory (no processing) or smart cards — May be used to generate static and dynamic passwords — Four kinds of smart cards:

      a.   <u>Static Password Tokens</u>: Owner authenticates himself to the token and token authenticates owner to the system.

      b.   <u>Synchronous dynamic password token</u>: Token generates a new unique password at fixed time intervals, users enters unique password and username into system, system confirms password and username are correct and entered during allowed time interval

      c.   <u>Asynchronous Dynamic PASSWORD Token</u>: same as synchronous, except no time dependency

     d.   <u>Challenge-Response Token</u>: system or workstation generates random number challenge, owner enters string into token along with proper PIN, token generates a response that is entered into the system

10.   **Single Sign-On (SSO)**: Kerberos, SESAME, KryptoKnight, and NetSP can provide SSO.

11.   **Kerberos**

> Dog in Greek mythology guarding gates of hell

> Software used in a network to establish user's identity

> Uses symmetric key encryption

> Users/systems are given tickets that can be used to identify themselves to other systems and secret crypto keys are provisioned for secure communications

> Three components: Key Distribution Center (KDC), Authentication Service (AS) exchange, and Ticket granting Service (TGS) exchange

> Single point of potential failure, susceptible to replay attacks during allotted time window

Four basic steps:

a.   KDC knows secret keys of all clients and servers on network;

b.   KDC initially exchanges information with the client and server by using the secret keys;

c.   Kerberos authenticates a client to a requested service on a server through the TGS, and by issuing temporary symmetric session keys for communications between the client and KDC, the server and the KDC, and the client and server; and

d.   Communication then takes place between client and server using those temporary session keys.

12.   **SESAME** — Secure **European** System for Applications in a Multi-vendor Environment — Addresses weaknesses in Kerberos by using <u>public key</u> cryptography for distribution of secret keys

13.   **KryptoKnight** — IBM developed, provides authentication, SSO, and key distribution services

14.   **Rule of Least Privilege**: Any object (user, administrator, program, system) should have only the least privileges the object needs to perform its assigned task, and no more

a. AC system grants user only those rights necessary for them to perform their work — Example, valet key v & overall key to car

b. Authorization creep occurs when someone continues to retain access privileges associated with a former position

c. Users should be re-authorized after each position change

15. **Accountability** is also important to access control — Ability to use log files and other accounting mechanisms to track users and their activities.

16. Methods of compensating for access control violations:

a. Backups

b. RAID

c. Fault Tolerance

d. Business Continuity Planning

e. Insurance

17. **Access Control Methodologies** — Access control can be divided into two categories:

a. Centralized Access Control: For dial-up users, the Remote Authentication Dial-in User Service (RADIUS) is used

(i) Callback can be used in RADIUS (beware hackers using call-forwarding)

(ii) Challenge Handshake Authentication Protocol (CHAP) is also used

(iii) For networked applications, the Terminal Access Controller Access Control System (TACACS) employees a user ID and a static password for network access — TACACS is unencrypted — TACACS+ uses two-factor authentication

b. Decentralized/Distributed Access Control: Use of databases to control access to information in a decentralized environment

VI. **CBK #6: Telecommunications and Network Security**

A. IDS – Not a preventive function

1. Network base – usually consist of network appliance with NIC operating in promiscuous mode to intercept packets in real time.

19

2. Host Based – small programs (agents) reside on host and monitor OS — Write log files and trigger alarms, only detects activity on host – not the network.

3. Knowledge-Based (Signature) – most common system — Low false alarms, resource intensive (continually update knowledge base), new or original attacks go unnoticed.

4. Behavior Based (Statistical anomaly) – Dynamically adapts to new vulnerabilities, high incidence of false alarms.

B. CIRT: (Computer Incidence Response Team) analysis of event notification; response to incident, escalation path, resolution and post-incident follow-up — Link user support and incident handling

C. RAID – Can be implemented in hardware or software — Three classifications of RAID, only Failure Resistant Disk Systems (FRDS) has been implemented — Ten levels of RAID — RAID level 5 is most popular implementation, stripes the data and parity information — RAID1 – mirroring and RAID0 – striping

D. Port Protection Device: Protects port from unauthorized use — Uses DES one-time PASSWORD challenge

E. Redundant servers (mirroring) versus Server Clustering (servers are managed as single system, all are online and working)

F. Cabling – exceeding effective length is problem

1. Coaxial – 50 ohm and 75 ohm — Baseband carries only one channel — Broadband carries several channels — BNC

2. Twisted pair — Wires can be shielded (STP) or unshielded (UTP) — Categories – the higher the category the more tightly wound the wire, giving greater protection from interference —RJ 45 — Category 5 is for fast Ethernet of 100 Mbps — STP used in Token Rings.

3. Fiber Optic – most resistant to interference — SC

G. LAN Transmission Methods: Unicast, multicast, broadcast

H. LAN Topologies: Bus, Ring, Star, Tree, and Mesh

I. Ethernet: 10BaseT is 10Mbps, 100BaseT is 100Mbps

Specification	Cable Type	Max Length
10BaseT	UTP	100 meters
10Base2	Thin Coax (Thinnet)	185 meters
10Base5	Thick Coax (Thicknet)	500 meters
10BaseF	Fiber	2000 meters

J. Network topologies

1. Ethernet

2. Token Ring

3. Fiber Distributed Data Interface (FDDI) – token ring passing media with dual rings.

K. Trivial File Transfer Protocol (tftp): use for saving setups and configuring files on routers and other devices — no security, use only with direct console connection

L. Trusted Network Interpretation (TNI) – Red Book

M. WAN

1. Private Circuit Technologies: dedicated line, leased line, PPP, SLIP, ISDN, DSL.

2. Packet Switched technologies: X.25, Frame Relay (fastest WAN protocol, no error correction), Asynchronous Transfer Mode (ATM) (data travels in fixed sizes called cells), Synchronous Data Link Control (SDLC, mainframe), High Level Data Link Control (HDLC, serial link), High Speed Serial Interface (HSSI) — More cost effective than dedicated circuits because they can create virtual circuits, where are used as needed.

3. Protocols:

a. High-level Data Link Control (HDLC) — Layer 2 — Uses frames

b. High Speed Serial Interface (HSSI) — Short distance, 50 feet

N. Remote Node Security Protocols:

1. Password Authentication Protocol (PAP, standard auth method, password and username sent in the clear) and CHAP

2. TACACS, TACACS+ (two factor ID) and RADIUS provide central db, which maintains user lists, passwords, user profiles that can be accessed by remote access equipment on the network — cannot provide two-way authentication

3. Systems are "standards-based" meaning they are interoperable with other systems of the same type

O. Data encapsulation is process in which information from one packet is wrapped around or attached to the data of another packet — In OSI model each layer encapsulates the layer immediately above it

P. Open Systems Interconnect (OSI) Model from International Standards Organization (ISO):

Layer 7 — Application – Confidentiality, authentication, data integrity, non-repudiation, gateways — FTP, SNMP, SMTP, DNS, TFTP, NFS, S-HTTP

Layer 6 — Presentation – Confidentiality, authentication, encryption, gateways

Layer 5 — Session – NO SECURITY, gateways — RPC and SQL

21

Layer 4 — Transport – Confidentiality, authentication, integrity — TCP and UDP — SSL, SSH-2, TLS

Layer 3 — Network – Confidentiality, authentication, data integrity, virtual circuits, routers — IP and IPSec — ARP, RARP, ICMP

Layer 2 — Data Link – Confidentiality, bridges, switch, HDLC — PPTP, L2F, and L2TP — Token ring and Ethernet — PPP and SLIP

Layer 1 — Physical – Confidentiality, ISDN, repeaters, hubs — Sends and receives bits — IEEE 802 and 802.2 — X.21 and HSSI

Q. DOD or TCP/IP Model

1. Application Layer

2. Host-to-Host — TCP and UDP

3. Internet — IP, ARP, RARP, IGMP and ICMP

4. Network Access (Link)

R. TCP versus UDP

TCP	UDP
Acknowledged	Unacknowledged
Sequenced	Subsequence
Connection-oriented	Connectionless
Reliable	Unreliable
High overhead	Low overhead (faster)

	TCP	UDP
Application Layer	Stream	Message
Host-to-Host Layer	Segment	Packet
Internet Layer	Datagram	Datagram
Network Access Layer	Frame	Frame

S. Security Protocols

1. Transport Layer Security Protocol (TLS)

   a. Can use with Kerberos and with PPP for authentication

2. Secure Shell (SSH)

   a. Host and user authentication, data compression, data confidentiality and integrity

22

3. Secure Sockets Layer (SSL)

   a. Client/server applications communicate securely

   b. Uses session keys for encryption

T. Firewalls Types: Basic default should be to deny all traffic unless expressly permitted

1. Packet Filtering (screening router) — Examines source and destination address of packet — Can deny access to specific applications or services based on ACL — First generation firewall — Operates at network or transport layer

2. Application Level Firewall (proxy server; application layer gateway) — Second generation — Reduces network performance — Circuit level firewall is a variation, creates virtual circuit between client and server (SOCKS)

3. Stateful Inspection Firewall — Third generation — Packets are captured by an inspection engine — Can be used to track connectionless protocols like UDP

4. Dynamic Packet Filtering Firewalls — Mostly used for UDP — Fourth generation

U. Firewall Architectures

1. Packet filtering routers

2. Screened host systems — Uses packet filtering router and a bastion host — Provides both network layer packet filtering and application layer proxy services

3. Dual Homed Host Firewalls — Single computer with two NICs, one connected to trusted network and other connected to Internet (or untrusted network)

4. Screened Subnet Firewalls — Two packet filtering routers and a bastion host — Provides DMZ

V. VPN — Creates secure communications link using a secret encapsulation method — Link is called a secure encrypted channel, more accurately an encapsulated tunnel, because encryption may or may not be used
Protocols:

1. Point to point tunneling protocol (PPTP) — Based on PPP — Dial in — Data link layer (Layer 2) — transmits over IP networks — connection oriented — an encryption protocol

2. Layer 2 Tunneling Protocol (L2TP) —Based on PPP and Layer 2 Forwarding (L2F) — Dial in — IETF wants L2TP to be standard — Data link layer (Layer 2) — can tunnel through networks that use non-IP protocols — has no encryption, but can combine with IPSEC for security — supports TACACS+ and RADIUS

3. IPSec — Used LAN to LAN — Network Layer (Layer 3) — Limited to IP — handles multiple connections at the same time — has functionality to authenticate and encrypt — needs Internet Key Exchange (IKE) to exchange

23

keys — cannot use with NAT because needs IP address — IPSec devices have two modes:

    a.   Tunnel mode – entire data packet is encrypted and encased in an IPSec packet

    b.   Transport mode – only the datagram is encrypted, not the header

W.   Network requirements: NIC, transmission medium (copper, fiber, wireless), NOS, and a LAN device to physically connect the computers (hub, bridge, router, switch)

X.   Repeater — Hub (concentrator) — Bridge forwards data to all other network segments — Switch sends data to specific port where destination MAC address is located — Router

Y.   CAN – Campus Area Network

Z.   Network Abuse Classes:

1.   Class A – Unauthorized access of restricted resources by circumvention of access controls by legitimate.

2.   Class B – Unauthorized use for non-business purposes.

3.   Class C -- Eavesdropping

4.   Class D – Denial of service or other service interruptions

5.   Class E – Network Intrusion

6.   Class F -- Probing

AA.   LAN

1.   Address Resolution Protocol (ARP) — Resolves 32-bit IP address to 48-bit Ethernet address

2.   Reverse Address Resolution Protocol (RARP) — Ethernet to IP address

BB.   Backup Concepts (must physically secure):

1.   Full — backups all files, modified or not and removes the archive attribute

2.   Incremental – backs up only those files that have been modified since the previous backup and removes the archive attribute

3.   Differential – backs up files that have been modified since last full backup and does not touch the archive attribute

CC.   Tape Formats

Properties	Digital Audio Tape (DAT)	Quarter Inch Cartridge (QIC) drives	8mm Tape	Digital Linear Tape (DLT)
Capacity	4GB/12GB	13 GB	20GB	20/35GB

Max transfer rate	1MBps	1.5MBps	3MBps	5MBps
Cost	Medium	Low	Medium	High

VII. **CBK #7: Cryptography.**

    A.   Cryptology is cryptography and cryptanalysis

        1.   Cryptography: science of codes

        2.   Cryptanalysis is science of breaking codes

    B.   History

        1.   Hieroglyphs in Egypt > 4,000 years ago

        2.   Scytale in Sparta 400 BC — paper wrapped around rod

        3.   Caesar cipher — 49 BC

        4.   Alberti's cipher disk — Italy in 1459 AD

        5.   Trithemius in 1518 AD — first book on cryptology & polyalphabetic ciphers

        6.   Grieppenstierna Cyphering Machine — Sweden in 1786 — enter plaintext and get out ciphertext

        7.   Thomas Jefferson — 1790 — ciphering device with 26 disks

        8.   Enigma machine used by Germany during WWII — 1933-1945

        9.   Japanese Purple Machine — 1937

        10.   IBM led by Dr. Feistel — 1970 — develops Lucifer ➜ DES

        11.   Diffie-Hellman public key cryptography — 1976

        12.   RSA in 1977

        13.   IDEA in 1990 to replace DES

        14.   PGP in 1991 — freeware

        15.   Rijndael announced winner of NIST AES in 2000

    C.   XOR: 0+0 = 0; 0+1 = 1; 1+0=1; 1+1=0

    D.   One time pad is usually implemented as a stream cipher using XOR function

    E.   **Work function** (factor): estimate of time needed to break a protective measure

    F.   **Link encryption** – individual application of encryption to data on each link of a network

    G.   **End-to-end encryption** – encryption of data from source system to end system

    H.   Security of cryptosystem should only depend on security of keys, not the algorithm

I. **Block code cipher**: message broken into blocks and each block encrypted separately — Blocks of identical plaintext have identical ciphertext — Replay and substitution attacks easier — DES is block cipher

J. Block chaining – parts of previous block are inserted into current block — Makes replay and substitution attacks harder

K. **Stream cipher** – message broken into characters or bits and enciphered with a key stream (random and independent of message stream) — XOR generally used — XOR key stream and message — XOR encrypted output with key stream a second time to decode — usually implemented in hardware

    1. Strong if (1) long period with no repeating, (2) functionally complex, (3) statistically unpredictable, (4) statistically unbiased, and (5) key stream not linearly related to key

L. Process of establishing a session key is called key exchange, negotiation, or distribution

M. **Symmetric Key Cryptography** — private key/secret key

    1. Single key shared by sender and receiver

    2. Rijindael, DES, Triple DES, Blowfish, IDEA, RC4, SAFER

    3. Strengths: 1,000 or more times faster than asymmetric

    4. Weaknesses: key management is a weakness – requires secure key distribution – not scalable to large numbers of users – does not provide authentication and non-repudiation services

N. **Asymmetric Key Cryptography** — public key

    1. Message encrypted with one of keys can be decrypted with other — two key pairs – private key (kept secret) and public key (made available)

    2. Based on difficult to solve problems – factoring the product of two large primes or discrete logarithm problem

    3. RSA, Diffie-Hellman, El Gamal, Elliptic Curve (ECC), Digital Signature Standard (DSS)

    4. Requires larger keys than symmetric (512 – 64; 1792 – 112)

    5. Strengths: efficient key distribution, scalable, provides confidentiality, access control, authentication, integrity, and non-repudiation services

    6. Weaknesses: very intense computations, slower than symmetric

O. **Hybrid Systems**

    1. Symmetric key for bulk data encryption

    2. Asymmetric key for key distribution

P. Terms

1. **Substitution ciphers** — shift alphabet or scramble alphabet and substituting characters

2. **Transposition cipher** — position of letters is permuted

3. **Polyalphabetic cipher** — use multiple substitution ciphers with different alphabets to defeat frequency analysis

4. **Running key cipher** — uses text from a source, such as a book, to encrypt the plaintext – key is known to sender and receiver – page, line, and character number

5. **One time pad** — key is a random set of non-repeating characters and each key bit is used only once — each key bit is XORed with message bit to produce ciphertext — each key bit is XORed with ciphertext to decrypt

6. **Concealment cipher** — message is hidden in another message – every so many words for example

7. **Steganography** — data hidden in picture files (least significant bits of bitmap image), sound files, slack space on disks

8. **Codes** — list of codes or phrases and their corresponding code group

9. **Machines** — Hagelin machine (combines plaintext with key stream to produce ciphertext), rotor machine uses rotors to produce cipher alphabet (Japan's Purple and Germany's Enigma)

10. **DES**: block cipher — symmetric key — 56 bit key, plus 8 parity bits — 16 rounds of transpositions and substitutions

    Four Modes:

    a. Electronic Code Book (ECB) — 64-bit data blocks processed at one time — same message and key produce same ciphertext

    b. Cipher Block Chaining (CBC) — first 64-bit plaintext block XORed with an initializing vector and processed with key to produce ciphertext which is then XORed with second 64-bit plaintext block to produce second ciphertext block, etc.

    c. Cipher Feedback (CFB) — first 64-bit plaintext block is XORed with the key-ciphered initialization vector to produce the ciphertext – this ciphertext is encrypted with key and XORed with second 64-bit plaintext block to product second ciphertext block, etc.

    d. Output Feedback (OFB) — similar to CFB except the XORed bits are not a function of either the plaintext of the ciphertext – initialization vector is used to seed the process – IV is DES encrypted and XORed with first data block to produce first ciphertext – the DES encrypted IV is DES encrypted again for the second block, etc.

11. **Double DES:** block cipher — symmetric key — 112 bit key — no more secure than DES

12. **Triple DES:** block cipher — symmetric key — 168 bit key — different modes:

    a.   3 DES encryptions with 3 different keys

    b.   Encrypt – decrypt – encrypt with three different keys

    c.   Encrypt – encrypt – encrypt with two different keys (first and third operation use same key

    d.   Encrypt – decrypt – encrypt with two different keys (first and third operation use same key

13. **International Data Encryption Algorithm (IDEA):** block cipher — symmetric — 128-bit key — 8 rounds of transpositions and substitutions — three mathematical functions: XOR, Addition mod 65536, and Multiplication mod 65537

14. **Rivest Cipher 5 (RC5)**: variable block size — symmetric — variable key size — data dependent rotations — variable number of rounds — primarily software implementation

15. **Advanced Encryption Standard (AES):** Rijndael Block Cipher — symmetric — variable block and key length (128, 192, 256)

16. **Public Key Cryptography:**

    a.   Uses one-way hash function for message integrity, time date stamp

    b.   Uses mathematical function that is easier to compute in one direction than in the opposite direction

    c.   *Trap Door One-Way Function*

        (i)   Forward direction takes seconds while inverse direction can take months to compute

        (ii)   Inverse is easy if have piece of information – trap door

        (iii)   Public key gives info about the function while the private key gives info about the trap door

17. **Secure Message:** w/asymmetric crypto, sender encodes message with receiver's public key and receiver decodes with private key — confidentiality

18. **Open Message:** w/asymmetric crypto, sender encodes message with sender's private key and receiver decodes with sender's public key — authentication and non-repudiation

28

19. **Secure and Signed Message:** w/asymmetric crypto, sender encodes message with own private key, sender re-encodes message with receiver's public key and receiver decodes with own private key and decodes again with sender's public key — authentication, non-repudiation, and confidentiality

20. **RSA:** (Rivest, Shamir, and Adleman) — asymmetric — factoring large prime integers — services: encryption, key distribution of symmetric keys, and digital signatures — 512-bit and 768-bit keys are weak, but 1024-bit key is moderately secure

21. **Elliptical Curve Cryptosystem (ECC):** asymmetric — based on mathematical problem of factors that are coordinate pairs that fall on an elliptical curve — services: encryption, key distribution of symmetric keys, and digital signatures — **highest strength per bit of public key systems**

22. **Diffie-Hellman:** first public key algorithm — patent expired in 1997 — key exchange algorithm

23. **El Gamal:** asymmetric — based on difficulty in calculating discrete logarithms in a finite field — services: encryption and digital signatures

24. **Merkle-Hellman Knapsack:** asymmetric — based on subset of sum problem in combinatorics — has been broken

Q. Time stamps can be used to prevent replay attacks

R. Elliptic curve – best bandwidth, computation, and storage — Wireless

S. Key escrow: Clipper chip with Skipjack algorithm (80 bit key, 64 bit block) — Key split in two and held by to escrows

T. **Digital Signature**: used to detect unauthorized modifications and authenticate sender — provides non-repudiation — private key signs and public key verifies — used to authenticate software, data images, users, machines

Steps:

1. Compute message digest

2. Digest is fed into digital signature algorithm with sender's private key to generate digital signature

3. Message and attached digital signature sent to recipient.

U. **Digital Signature Algorithm (DSA):** Digital Signature Standard (DSS) — uses secure hash algorithm (SHA-1) and condenses message to 160 bits — Key size 512 to 1024

V. **Hash Function**:

1. Condenses arbitrary length messages to fixed length – usually for subsequent signing by a digital signature algorithm

2. Output is message digest, Two files cannot have same hash, Can't create file from hash

3. MD5 – 128 bit digest of input message, uses blocks of 512, 4 rounds of transformation

4. SHA-1 (by NIST) — SHA-256, SHA-384, SHA-512 supports AES — HAVAL

5. HMAC — hashed MAC more secure and more rapid message digest

W. **Message Authentication Code (MAC)**: used when sender only wants one person to be able to view the hash value – the value is encrypted with a symmetric key — similar to a CRC — weak form of authentication

X. Clustering: plaintext message generates identical ciphertext using the same transformation algorithm, but with different keys (cryptovariables) —

Y. **Certificate Authority (CA)**: binds public key to person — Certificate revocation list — X.509 provides format for digital certificates.

Z. **Privacy Enhanced E-mail (PEM)**: Proposed by IETF to comply with Public Key Cryptography Standards (PKCS) developed by Microsoft, Novell and Sun — Uses MD2/MD5 for message digest, DES-CBC or triple DES-EDE for text encryption and RSA for digital signature and key distribution — certificates based on X.509

1. Privacy, message integrity, authentication and non-repudiation

AA. **Pretty Good Privacy (PGP)**: message privacy for stored files, email, file attachments — random prime numbers + passphrase

1. Privacy, integrity, identification authentication, and policy enforcement

2. Symmetric encryption — 3DES, DES, IDEA

3. RSA, DSS, and Diffie-Hellman for the symmetric key exchange

4. SHA-1 and MD5 for hashing

5. Web of trust instead of CA

BB. Attacks on Symmetric Block Ciphers

1. Differential Cryptanalysis — private key cryptography — looks at ciphertext pairs with specific differences and analyzes the effects of these differences

2. Linear Cryptanalysis — uses known plaintext and corresponding ciphertext to generate a linear approximation of a portion of the key

3. Differential Linear Cryptanalysis — combination of both

4. Algebraic Attacks — relies on block ciphers displaying high degree of mathematical structure

VIII. **CBK #8: Applications and Systems Development.**

A. Software development models:

1. Simplistic

2. Waterfall (limited to one stage of re-work), Modified Waterfall (phases end on milestones)

3. Spiral (four quadrants: requirements, objective, planning, risk analysis)

   a. Angular dimension is progress made in completing project

   b. Radial dimension is cumulative cost of project

   c. Using live data is not appropriate — Live data may not exercise all functions, including out of range and other invalid types — Testing should not be done by the programmers

B. Maintenance phase: request control, change control, and release control.

C. Configuration Management: British Standards Institute 7799: tracking and issue of new versions

   1. A configuration item is a component whose state is to be recorded and against which changes are to be progressed

   2. Configuration control controls changes to the configuration items and issues versions of the items from the software library

   3. Two goals: (1) ensuring changes to system do not unintentionally or unknowingly effect security; and (2) ensuring changes to system are reflected in documentation

D. Software cycle:

   1. Verification: evaluate product in development against the specification.

   2. Validation: Evaluate against real-world requirements and concepts.

E. Software Capability Maturity Model (CMM): Quality software is a function of the quality of its associated software development and maintenance process — level 3 requires ISO 9001

F. Software Development Life Cycle:

   1. Project Initiation and Planning:

Activities	Parallel Security Activities
Identify user needs	Identify security needs
Evaluate alternatives	Initial risk analysis
Select/approve approach	Identify security framework

   2. Function Requirements Definition

Activities	Parallel Security Activities
Prepare project plan	Insert security areas into project plan
Develop functional requirements	Define security requirements Risk analysis & Contingency Plan

Preliminary test plans	Preliminary security test plans
Select acquisition strategy	Include security requirements in RFPs and contracts
Establish formal functional baseline	Functional baseline includes security requirements

3.   System Design Specifications

Activities	Parallel Security Activities
Develop detailed design	Define security specifications
Update testing goals and plans	Update security test plans
Establish formal baseline	Formal baseline must include security areas

4.   Develop and Document

Activities	Parallel Security Activities
Construct from detailed design specification	Write/procure and install security related code
Perform and evaluate unit tests	Perform unit tests Evaluate security code
Implement detailed design	Include approved security components in formal baseline

5.   Acceptance Testing

Activities	Parallel Security Activities
Test system components	Test security components
Validate system performance	Test security in integrated system
Perform acceptance test on implemented system	Conduct acceptance test
Accept system	Verify project security

6.   Implementation

Activities	Parallel Security Activities
Install system	Install security code

Prepare project manuals	Document security controls

      7.   Operations and Maintenance Support

G.   Database: manage information from many different sources

H.   Database Management System (DBMS): manages large structured sets of data, provides multiple users access, security, and controls, enforces the integrity of the data, provides for fault tolerance

      1.   Models

          a.   Hierarchical

          b.   Network

          c.   Relational database models

               (i)   Three parts: (1) data structures called tables or relations; (2) Integrity rules on allowable values and value combinations in the tables; and (3) operators on the data in the tables

               (ii)   Fundamental entity is the relation (table or set of columns in table)

               (iii)   With "attributes" (columns), having permissible values, specific attribute is "key" with unique values, occurring in "instances" or tuples (rows

               (iv)   Cardinality is # of rows

               (v)   Degree is # columns

               (vi)   Primary key is unique identifier in table that points to tuples; subset of candidate keys

               (vii)   Candidate key is an attribute that is a unique identifier within a given table

               (viii)   If attribute in one relation has values that match primary key in another relation, this attribute is called a foreign key

               (ix)   Security is provided through views

               (x)   Description of the database is called a schema, which is defined by the Data Description Language (DDL)

               (xi)   Primary key is chosen from set of candidate keys

(xii)   A domain of a relation is the set of allowable values that an attribute can take on

(xiii)   Relational is used for information in text form

2.   Graphics, video, and multimedia are more suited to an Object-Oriented Data Base (OODB)

3.   There is also the hybrid, called the object-relational DB

4.   Integrity

      a.   Entity integrity — primary key is unique and no null keys

      b.   Referential integrity — foreign key is a primary key in another table and no null foreign keys

I.   Object Oriented Systems: more reliable and capable of reducing propagation of change errors — Dynamic objects are created during program execution

1.   Objects are encapsulated – only access through messages sent to them to request performance of their desired operations

2.   Substitution property: objects with compatible operations can be substituted for each other

3.   Message is a communication to an object

4.   Behavior is the results exhibited by an object on receipt of a message

5.   Class is collection of common objects

6.   Method is the code that defines the actions an object performs in response to a message

7.   Inheritance – methods from a class are inherited by members of its subclasses

8.   Delegation is forwarding a request from one object to another

9.   Polymorphism is objects of many different classes that are related by some common superclass; thus any object denoted by this name is able to respond to some common set of operations in a different way

10.   Polyinstantiation is development of a new version of an object from another object replacing variables with other values

      a.   For example, relational database, the name of a military unit may be classified in the database and may have an ID # as the primary key. If another user at a lower classification level attempts to create a confidential entry for another unit using the same id# as a primary key, a rejection of the attempt would infer to the lower level user the same ID exists at a higher classification.

      b.   To avoid inference, systems will allow same id# for lower class and the DBMS would manage to permit same primary key for two different units

   c. Prevents inference violations

J. Jargon

 1. Open Database Connectivity (ODBC)

 2. Object Link and Embedding DB (OLE DB)

 3. Active-X Data Objects (ADO)

 4. Java Database Connectivity (JDBC)

 5. Distributed Component Object Model (DCOM)

K. Objects can be made available to users through Object Request Brokers (ORBs) — ORBs are middleware because they reside between two other entities — establishes client/server relationship between objects

L. Common Object Request Broker Architecture (CORBA) defines standard that enables programs written in different languages and using different platforms and operating systems to interface and communicate —

M. Artificial Intelligence (AI):

 1. Expert Systems: acts like a human expert — Builds knowledge base (in the form of If-Then statements) of the domain to be addressed in the form of rules and an inference mechanism to determine if the rules have been satisfied by system input — Inference engine + knowledge base = expert system — Fuzzy logic used to address uncertainty.

 2. Neural Networks: Neurons, signals are exchanged among neurons through electrical pulses traveling along an axon — Electrical pulse arrives at a neuron at points called synapses — Output = Input1*Weight1 + Input2*Weight2 — Summation of inputs with dynamic weights assigned to them — One summing node is called a single-layer network — Multiple summing nodes is a multi-layer network — Training develops the weights

N. Database security issues

 1. Granularity of the access to objects in DB refers to fineness with which access can be controlled or limited

 2. Aggregation is act of obtaining info of a higher sensitivity and combining it with lower levels of sensitivity

 3. Inference is ability of users to infer or deduce info about data at sensitivity levels for which they do not have access — A link that enables an inference to occur is called an inference channel

O. DBMS Controls

 1. Atomicity — either all changes take effect or none

 2. Consistency — a transaction is allowed only if it follows owner or system-defined integrity constraints

3. Isolation — the results of a transaction are not visible until the transaction is complete

4. Durability — the results of a complete transaction are permanent

5. Concurrency controls — ensure that two users cannot simultaneously change the same data

6. Knowledge Discovery in Databases (KDD) — a method of identifying valid and useful patterns in data

    a. Probabilistic approach — based on probability and data interdependencies

    b. Statistical approach — based on data relationships

    c. Classification approach — based on grouping data according to similarities

    d. Deviation and Trend Analysis — uses filtering techniques to detect patterns

    e. Neural Networks — organizes data into nodes that are arranged in layers — links between nodes have specific weighting classifications

    f. Expert system approach — uses knowledge base and algorithms and/or rules that infer new facts from knowledge and incoming data

    g. Hybrid approach — combines two or more approaches

P. Data Warehouse and mining:

1. Data warehouse is a repository of info from heterogeneous databases

2. Objective is to find relationships that were unknown up until now among data in warehouse — called data mining

3. Correlations or data about data is called metadata — Metadata not stored in data warehouse, instead stored in a highly protected "data mart."

4. Data warehouse and mining can be applied to audit logs and other info to find system anomalies

Q. Data Dictionary: database for developers, records all the data structures used in an application

R. Accreditation: Formal acceptance of security adequacy, authorization for operation and acceptance of existing risk

S. Certification: Formal testing of security safeguards

T. Operational assurance: verification system is operating to its security requirements — Look at policies, audits, and system monitoring

36

U. Distributed environments permit agents — Agents are surrogate programs or process performing services in one environment on behalf of a principal in another environment — Not a proxy, which hides identity

V. Distributed systems should include:

   1. Interoperability

   2. Portability — Software at source code level can be moved from system to system with different vendors

   3. Transparency — Ability to keep application and its processes invisible to the end user

   4. Extensibility — System must be able to adapt to various management policies and allow introduction of new resources to manage

W. Single state machines can only process one security level at a time — Multi-State Machines can process two or more security levels at the same time

X. Interpreted language executes each instruction in real-time, called run-time binding — Compiled language, binding occurs at compile time — Compiled code poses greater security risk since it may contain destructive code that can't easily be detected

Y. Applets in Web browsers called mobile code — Java runs in constrained memory space (sandbox) for security

Z. Security measures: configure firewalls to screen applets; configure browsers to restrict or prevent downloading applets; permit applets only from trusted parties, provide training to users re mobile code

Application control type	Accuracy	Security	Consistency
Preventive	Data checks, forms, custom screens, validity checks	Firewalls, sensitivity labels, encryption, passwords, test environments	Data dictionary, programming standards
Detective	Hash controls, cyclic redundancy checks	IDS and audit trails	Comparison controls, relationship tests
Corrective	Backups, checkpoint restarts	Emergency response and reference monitor	Program comments and database controls

IX.   **CBK #9: Physical Security.**

A. Five threats: interruptions in computing services, physical damage, unauthorized disclosure of information, loss of control of system integrity, and physical theft

B. **Administrative Controls**: proper emergency procedures, policy implementation, facility security management (audit trails and emergency procedures), pre-employment screening, on-going employee checks, post-employment procedures — Audit trails and access logs are detective, not preventative

    1. **Facility Requirements Planning**

        a. Choosing a facility that is secure

            (i) Visibility

            (ii) Local considerations — near hazards, dump, high crime rate

            (iii) Transportation

            (iv) Natural disasters — floods, earthquakes, wind, snow

            (v) Joint tenancy

            (vi) External services — hospital, fire station, police

        b. Designing a secure site

            (i) Follow local building codes and other regulations

            (ii) Ceilings, floors, sprinkler systems, liquid or gas lines, air conditioning, electrical

            (iii) Doors — solid core vs. hollow core, hinges, contact devices, doorframe vulnerabilities, location, numbers

            (iv) Windows — types of glass, location

            (v) Walls — interior walls should be floor to ceiling

    2. **Facility Security Management**

        a. Audit or access logs

            (i) Data and time access attempted

            (ii) Whether successful or not

            (iii) Location of access attempt

            (iv) Who attempted entry

            (v) Who modified access privileges to allow entry

      b.   Emergency procedures

           (i)   Emergency system shutdown procedures

           (ii)   Evacuation procedures

           (iii)   Employee training, awareness programs, and periodic drills

           (iv)   Periodic equipment and systems tests

3. **Administrative Personnel Controls** – usually administered by HR

      a.   Pre-employment screening — employment, references, and educational history checks, background investigations, credit rating checks

      b.   On-going employee checks — security clearances, on-going ratings and reviews by supervisor

      c.   Post-employment procedures — exit interview, removal of network access and change of passwords, return of computer inventory and laptops

C. **Environmental and Life Safety Controls**:

1. **Electrical Power**:

      a.   Noise — (EMI, RFI), use power line conditioning, proper grounding, cable shielding, limiting exposure to magnets, fluorescent lights, electric motors, and heaters

      b.   Humidity — range should be 40-60% — <40% increases likelihood of static electricity — >60% increases condensation

           (i)   Hygrometer to measure humidity

      c.   Static electricity controls: anti-static sprays, antistatic flooring, proper grounding, anti-static table or floor mats, HVAC to control humidity

      d.   Power vulnerabilities

           (i)   Blackout is prolonged power loss

           (ii)   Fault is momentary power loss

           (iii)   Brownout is prolonged period of low voltage

           (iv)   Sag/Dip is momentary period of low voltage

           (v)   Surge is prolonged high voltage

(vi)   Spike is momentary high voltage

(vii)   Inrush current is initial surge of power at the beginning

(viii)   Noise is steady interfering disturbance

(ix)   Transients are line noise disturbances of short duration

(x)   Electrostatic discharge is another type of electrical surge

e.   EPO – Emergency Power Off — Air conditioning should have separate EPO

f.   Methods to protect power: UPS, power line conditioning, backup power sources, surge suppressors, alternate power source, dedicated feeders and circuits

2.   **Fire detection and suppression**

a.   Three elements – oxygen, heat, and fuel

(i)   Water suppresses temperature

(ii)   Soda acid reduces fuel supply

(iii) CO_2 (lethal if removes all O_2) reduces oxygen

(iv)   Halon suppresses combustion through a chemical reaction that kills the fire

b.   Fire Detectors

(i)   Heat sensing — temperature reaches a certain temperature or sudden rise in temperature

g)   Fixed or rate-of-rise temperature sensors

(ii)   Flame actuated — expensive — sense either the infrared energy or pulsation of the flame

(iii)   Smoke actuated — primarily in ventilation systems

h)   Ionization — detects charged particles in smoke

i)   Photoelectric — variation in light blockage caused by smoke

(iv)   Automatic dial-up — dials up local fire and/or police station and plays a recorded message — used in conjunction with other detectors

     c.   Fire extinguishing systems

         (i)   Wet pipe — water in pipes at all the time

         (ii)   Dry pipe — water in pipes only when activated

         (iii)   Deluge — type of dry pipe, but amount of water discharged is much greater

         (iv)   Preaction — dry until heat, then loads water, releases water flow when link in nozzle melts; most recommended for computers

         (v)   Gas discharge systems

              j)   Employ pressurized inert gas usually from under raised floor — CO_2 and Halon

                  i)   Halon now listed as danger to ozone and is being phased out

                  ii)   Halon not safe above 10% concentration — Use in > 900 degrees creates toxic gas

                  iii)   Halon 1211 (portable extinguishers) and Halon 1301 (flooding systems)

                  iv)   FM-200 is good replacement — Fire contaminants: smoke, heat, water, suppression medium contamination (CO_2 or Halon)

     d.   Sprinklers do not cause water damage – fire does — Sprinklers protect lives, reduce fire damage, limit fire to building

     e.   Fire distinguishers should be 50 feet from equipment and toward the door.

Class	Description	Suppression Medium
A	Common combustibles	Water or soda acid
B	Liquid	CO_2, soda acid, Halon
C	Electrical	CO_2 or Halon
D	Combustible metals	Dry powder

3.   **Heating, Ventilation, and Air Conditioning (HVAC)**

     a.   Turn off in event of fire

41

D. **Physical and Technical Controls**

1. Facility Control Requirements

   a. Guards — expensive, can make value decisions/discriminating judgment

   b. Dogs — expensive, loyal, keen sense of smell

   c. Landscape — can provide barrier as long as provide bridge over a fence

   d. Fences — primary means of perimeter or boundary protection — fences, gates, turnstiles, bollards

      (i) Mantrap — physical access control routed though a set of double doors that may be monitored by a guard

3' to 4' (1 meter)	Deters casual trespasser
6' to 7' (2 meters)	Too hard to climb easily
8' with 3 strands of barbed wire (2.4 meters)	Deters intruders

   e. Lighting — NIST STD – 8 feet high with 2 foot candle — continuous lighting, glare lighting, trip lighting, standby lighting, emergency lighting

   f. Locks — most accepted and used physical security device; can be picked

      (i) Combination locks, deadbolt locks, keyless locks, smart locks

   g. Closed Circuit TV (CCTV) — television transmission system that uses cameras to transmit pictures

      (i) CCTV Levels — detection, recognition, identification

      (ii) Camera, monitor, transmission media

      (iii) Lighting is important

   h. Guard Stations — posted at visitor and employee entrances — deterrence

2. Facility Access Control Devices

   a. Security Access Cards

      (i) Photo-image cards — ID card with picture

          (ii)   Digital coded cards — magnetic strip requires reader; smart entry card with magnetic stripe or integrated circuit chip may require PIN; smart card with authentication token to generate one-time or challenge response password or PIN

          (iii)   Wireless proximity readers

               k)   User activated transmits a sequence of keystrokes to wireless keypad

               l)   System-sensing proximity

                    i)   Passive — senses electromagnetic field of reader

                    ii)   Field-powered — contains active electronics, RF transmitter and power supply

                    iii)   Transponder — reader interrogates card which transmits an access code

    b.   Biometric devices — see access control

3.   Intrusion Detection and Alarms

    a.   Should be installed on doors, windows, ceilings, walls, roofs, ventilation openings, etc

    b.   Alarms must be audible for at least 400 feet

    c.   Perimeter — photoelectric sensors, dry control switches

    d.   Motion Detectors — wave pattern, capacitance (electrical field surrounding an object), audio detectors

    e.   Alarm systems — local alarm system, central station systems, proprietary system, auxiliary station system

4.   Computer Inventory Control

    a.   PC Physical Control — cable locks, port controls, switch controls, peripheral switch controls, electronic security boards

    b.   Laptop Control

5.   Media Storage Requirements

    a.   Object reuse: reusing data storage media after initial use.

    b.   Data Remanence: residual info remaining on media after erasure, which may be restored — Orange Book requires magnetic media be

formatted seven times before discard or reuse — Common problems with media erasure:

> (i)   Deleting does not actually remove data, file allocation table

> (ii) Damaged sectors may not be overwritten by format utility — Need degaussing.

> (iii) Improper use or equipment failure of degaussers

c.   Clearing: overwriting data on media for reuse within same secured environment (i.e., not used in a lesser security environment)

d.   Purging: degaussing or overwriting media to be removed from monitored environment, such as resale, use in unsecured environment, or donation

e.   Destruction: completely destroying media — Good practice to purge media before submitting for destruction

X.   **CBK #10: Law, Investigation, and Ethics**

A.   **Liability** — senior executives can be held liable for losses

1.   1997 Federal Sentencing Guidelines

a.   Extended to cover computer crimes and specified that senior corporate officers could be personally subjected to up to $290 million in fines if their organizations did not comply with the law

2.   Must exercise *due care* or *reasonable care* to carry out their responsibilities to their organization — must meet certain requirements to ensure corporate security

3.   Exercises *due diligence* — company kept up with these practices in a disciplined way rather than doing them once and letting them fall out of date and become useless

4.   Criteria for evaluating legal requirements for implementing safeguards is to evaluate cost (C) of instituting protection versus estimated loss (L) resulting from exploitation of vulnerability — If C<L, then liability

B.   **Major Legal Systems in the World**

1.   Common Law — developed in England — based on tradition, past practices, and legal precedents set by courts through interpretation — innocent until proven guilty — United States, United Kingdom, Australia, and Canada

2.   Civil Law or Code Law — fractured into separate national systems around the time of French Revolution — guilty until proven innocent — France, Germany, Quebec

3. Socialist Legal Systems — based on concepts of economic, political and social policies of the state — communist and socialist countries

4. Islamic and other Religious Law — law of the clergy, of belief systems, religions, and secret societies — special rights to clergy over common people

C. **Major Legal Systems in North America**

1. Criminal Law — Laws about individual conduct that violates government laws enacted for the protection of the public — punishment can include imprisonment, financial penalties, loss of right to work with computers

2. Civil (tort) Law — Laws about a wrong inflicted upon an individual or organization that results in damage or loss — punishment can include financial penalties or compensatory damages — NO imprisonment

3. Administrative/Regulatory Law — Standards of performance and conduct expected by government agencies from industries, organizations, officials, and officers — punishment can include imprisonment and/or financial penalties

D. **Intellectual Property** — typically includes at least four types of laws:

1. Patent — Provides the owner of the patent with a legally enforceable right to exclude others from practicing the invention covered by the patent for a specifies period of time — 17 years in US

2. Trademark — Establishes a word, name, symbol, color, sound, product shape, device, or combination of these that will be used to identify goods and to distinguish them from those made or sold by others

3. Copyright — Protects "original works of authorship" — Protects the expression of ideas rather that the ideas themselves

4. Trade Secrets — Secures and maintains the confidentiality of proprietary technical or business-related information that is adequately protected from disclosure by the owner

E. **Privacy Laws** — Protection of information on private individuals from intentional and unintentional disclosure or misuse

1. Includes information privacy, medical records, communications privacy

2. Globalization — distribution of information worldwide

3. Transborder Data Flow — how different countries provide privacy protection

4. Convergent Technologies — technical means of gathering, analyzing, and distributing information

5. Data Retrieval Advances — data warehouses and other types of repositories for personal information

6. European Union (EU) has more restrictive privacy laws than the United States — Prohibits transfer of personal information to locations when equivalent personal protections are not in place — data collected fairly and legally, accurate and kept current, cannot be disclosed without individual's permission

45

7. ***Organization for Economic Cooperation and Development (OECD) Guidelines of 1980*** — provides for data collection limitations, the quality of the data, specifications of the purpose for data collection, limitations on data use, information security safeguards, openness, participation by the individual on whom the data is collected, and accountability of the data controller

8. ***US Electronic Communications Privacy Act of 1986*** — prohibits eavesdropping or interception of message contents without distinguishing between private or public systems

9. ***Health Insurance and Portability Accountability Act (HIPAA) of 1996*** (Kennedy-Kassenbaum Act) — addresses the issues of personal health care information privacy and health plan portability in the United States

10. ***Gramm Leach Bliley (GLB) Act of 1999*** — requires financial institutions to develop privacy notices and give their customers the option to prohibit the banks from sharing their information with nonaffiliated third parties

11. **Privacy Act of 1974**: Federal agencies must protect information of private individuals in their databases

12. Monitoring can infringe on privacy — employee electronic monitoring, email monitoring, document monitoring, Internet activity monitoring

    a. Ensure proper policies are in place and employees are aware of the monitoring

    b. Monitor only work-related activities

    c. Consistent monitoring usage applied to all employees — no targeting a few

13. Protect personally identifiable information

F. **Differences in International Computer Crime Laws**

1. Different views on seriousness of computer crime (not seen as a threat in some countries) — law enforcement technical skills vary — different interpretations on technology issues

G. Investigation

1. Terms

    a. Incident — adverse event or series of events that impact an organizations security or ability to do business

    b. Event — an observable occurrence

2. Modus Operandi — examine to determine if suspect could have committed crime — criminal profiling

3. Because development of technology may outpace law, crimes of embezzlement, fraud, and wiretapping are frequently used

4. Companies should have an incident response policy and procedures to handle this type of event **before** it actually takes place

5. **Steps in Incidence Handling**:

   a. Report of cybercrime should be investigated to determine if an actual crime has been committed

   b. Senior management should be informed immediately of a cybercrime

   c. Contain the incident

   d. Analyze logs, audit trails, and gather information

      (i) Start documenting events along with the company employees and resources involved

      (ii) Decide whether to conduct own forensics or call in experts

      (iii) Determine when to call in law enforcement

   e. Track down the source of the incident

   f. Repair the damage and recover the environment

   g. Prevent similar incidents

6. ***Computer forensics*** — investigating computer crime — Collecting information from and about computer systems that is admissible in a court of law

   a. Chain of custody — A history that shows how the evidence was collected, analyzed, transported, and preserved in order to be presented as evidence in court — accountability

H. Evidence:

   a. Sources of evidence — oral, written, computer generated, visual/audio

1. Legal evidence

   a. ***Best evidence*** — original or primary evidence rather than a copy of duplicate of the evidence

   b. ***Secondary evidence*** — a copy of evidence or oral description of its contents; not as reliable as best evidence

   c. ***Direct evidence*** — proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses

47

d.   ***Conclusive evidence*** — incontrovertible; overrides all other evidence

e.   ***Opinions*** — two types: *Expert* — may offer an opinion based on personal expertise and facts, *Non-expert* — may testify only as to facts

f.   ***Circumstantial evidence*** — inference of information from other, immediate, relevant facts

g.   ***Corroborative evidence*** — supporting evidence used to help prove an idea or point; used as a supplementary tool to help prove a primary piece of evidence

h.   ***Hearsay evidence (3rd party)*** — oral or written evidence that is presented in court that is second hand and has no firsthand proof of accuracy or reliability

   (i)   Usually not admissible in court

   (ii)   Computer generated records and other business records are in hearsay category

   (iii)   Certain exceptions to hearsay rule (1) Made during the regular conduct of business and authenticated by witnesses familiar with their use (2) Relied upon in the regular course of business (3) Made by a person with knowledge of records (4) Made by a person with information transmitted by a person with knowledge (5) Made at or near the time of occurrence of the act being investigated (6) In the custody of the witness on a regular basis

2.   Standards for evidence

   a.   ***Relevant*** — must be related to the crime

   b.   ***Legally Permissible*** — evidence was obtained in a lawful manner

   c.   ***Reliability*** — evidence has not been tampered with or modified

   d.   ***Sufficient*** — must be persuasive enough to convince a reasonable person of the validity of the findings

   e.   ***Identification*** — evidence is properly identified without changing or damaging the evidence

   f.   ***Preservation*** — evidence is not subject to damage or destruction

3.   Evidence life cycle: collection and identification; analysis; storage, protection, transportation; presentation in court; and return to victim/owner

I. The extension of property to include electronic information has been key to the development of computer crime laws in some countries

J. FBI and Secret Service are responsible for computer crimes

K. Computer Incident Response Team (CIRT)

L. Enticement: intruder lured to certain system or selected files (honeypot)

M. Entrapment: encourages a person to commit a crime

N. Federal Computer Security Act of 1987: first to require government agencies to do security training and adopt security plan

O. **MOM**: Motive, opportunity and means

P. Typical computer felon holds a position of trust with the company

Q. **Ethics** — The analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology

    1. Ethics code does not include "control" as a behavior

    2. **(ISC)^2 Code of Ethics** — contains four cannons and some additional guidance under the Objectives for Guidance

        a. Conduct in highest standards of moral, ethical, and legal conduct.

        b. Not commit unlawful or unethical act that would negatively impact professional reputation or reputation of profession.

        c. Report unlawful activity and cooperate in investigation.

        d. Support efforts to promote prudent info security measures

        e. Provide competent service, avoid conflicts of interest

        f. Execute responsibilities to highest standards of profession

        g. Not misuse information they come in contact with, maintain confidentiality.

    3. **Internet Activities Board (IAB):** Unethical to:

        a. Seek unauthorized access to Internet resource

        b. Destroy integrity of information

        c. Disrupt Internet use

        d. Waste resources

        e. Compromise privacy of users

           f.   Negligence in Internet experiments

XI. **Types of Attacks/Threats**

A. Birthday: applied to the probability of two different messages having the same hash function that produces a common message digest

B. Brute Force: trying every possible combination of key patterns

C. Buffer overflow: process receives more data than expected and acts in an unexpected way

D. Chosen Ciphertext: portions of ciphertext are selected for trial decryption while having access to the corresponding decrypted plaintext

E. Chosen Plaintext: chosen plaintext is encrypted and output ciphertext is obtained

F. Ciphertext Only: only ciphertext is available

G. Corruption/modification: altering information or software

H. Covert Channel: Unapproved communications link between one application and another — Covert storage channel — Covert timing channel — asynchronous

I. Data diddling: changing data either before or after it enters the system

J. Data Remanence: residual info remaining on media after erasure, which may be restored

K. Demon (war) dialing: dialers automatically test every phone line in an exchange looking for modems that are attached to the network

L. Denial of Service (DoS): person, process, or other system consumes the resources (memory, storage, communications) of a system

M. Destruction: destroying information or hardware/software

N. Disclosure: release of information to unauthorized person(s)

O. Distributed Denial of Service (DDoS): extension of DoS, which gets more computers in the act — attacker creates master controllers that control slave or zombie machines

P. Dumpster diving: obtaining sensitive data by sorting through garbage in dumpsters or at recycling locations

Q. Emanation eavesdropping: receipt of information by intercepting RFI signals

R. Embezzlement: illegally acquiring funds, usually through manipulation and falsification of financial statements

S. Espionage:

T. Executable Code/Mobile Code: code that is downloaded to a user's machine and executed and could give the program access to unexpected resources on the machine

U. Garbage collection: a process that de-allocates storage during program execution

V.   Interruption: causing information, software, hardware, and/or telecommunications to become unavailable

W.   IP spoofing: impersonation of a computer from a trusted network.

X.   Known Plaintext: have sample of ciphertext and corresponding plaintext

Y.   Malicious code: programs such as Trojan Horses, worms, and viruses that cause DoS or destruction of information on computers

Z.   Man-in-the-Middle: takes advantage of store-and-forward nature of most networks by intercepting messages and forwarding modified versions of the original message

AA.   Meet-in-the-Middle: applied to double encryption schemes by encrypting known plaintext from one end with every possible key and comparing the results in the middle with the decryption of the corresponding ciphertext and each possible key

BB.   Network intrusions: unauthorized penetration into network computer resources

CC.   Network Packed Sniffers: software that uses a NIC in "promiscuous mode" to review packets sent across the network

DD.   Object reuse: reusing data storage media after initial use.

EE.   Password theft: through eavesdropping, sniffing, social engineering, man-in-the-middle attacks

FF.   Piggy-backing: an attacker gains unauthorized access by a system by using a legitimate user's connection

GG.   Ping of Death: (DoS) large PING packet attack

HH.   Port Scanning: scans to see what ports are open — nmap

II.   Social engineering: using social skills to get information

JJ.   Software piracy: illegal copying and use of software

KK.   Smurf: (DoS) IP spoofing (forged return address of target) with ICMP (PING) to saturate target network with traffic

LL.   Sniffing: protocol analyzer configured to capture data packets that are later decoded to collect information such as passwords and infrastructure configurations

MM. Spoofing (Masquerading): used to convince a system that it is communicating with a know entity — IP spoofing, fake login screen,

NN.   SYN: (DoS) exploits the TCP session initialization handshake by sending SYNs which fill up the systems small in-process queue

OO.   Teardrop: (DoS) hacker modifies the length and fragmentation offset fields in sequential IP packets

PP.   Theft/removal: loss of information or equipment

QQ.   Time of Check/Time of Use (TOC/TOU): exploits the difference in time that security controls were applied and the time the authorized service was used

RR. Trap door/back door: hidden mechanism that bypasses user authentication and other security measures that could enable unauthorized access

SS. Trojan Horses: contained in useful programs and performs unauthorized functions when triggered

TT. Viruses:

1. Program virus — attacks files that contain computer code

2. Boot virus — attacks boot sector on hard or floppy disk

3. System virus — attacks BIOS command and other system files

4. Polymorphic virus — changes as it replicates

5. Multipartite virus — infects in more than one place

6. Macro virus — contained in data files (word documents)

XII. **PKI**

A. Can be open (third party trusted CA for many organizations and individuals) or closed (CA and members are part of single organization)

B. CA – Certificate Authority; RA – Registration Authority; CRL – Certificate Revocation List; Certification Practice Statement (CPS), dictates legal responsibilities, roles, policies, and procedures for the CA

C. Services: confidentiality, access control, integrity, authentication, and non-repudiation

D. Manages generation and distribution of key pairs, publishes public keys, provides high degree of confidence

E. Certification is process of binding a public key to a specific person, entity, or system

F. Key recovery – key escrow

G. Public Key Cryptography Standards (PKCS) — PKCS#1 is RSA standard — PKCS#13 is elliptic curve crypto.

XIII. **Security Assessment**

A. Two parts: Physical and Logical

B. Areas of Review

1. Physical access: Access zones, server room access, backups, media, computers (laptops), network access

2. Network

3. Software

4. Messaging

5. Acceptable Use

6. Application Security

7. Data security/classification according to sensitivity or worth

8. Encryption

9. Change Control Systems

10. Disaster Recovery: storage of media; time to restore; test restores; encrypt

11. Incident response policy/team

12. User Training

13. Customer/Partner Training

XIV. **Security Tools**

A. Microsoft Passport — Internet directory service for authentication — Target consumer market

B. iChain by Novell — Uses Novell Directory Services (NDS) for storage of authentication data — Target business market

C. Firewall: Hardware or software that controls access to applications on a network — Three main types:

1. <u>Packet Filtering or screening routers</u> — Filters IP addresses by either allowing access to known IP addresses or denying access to IP addresses and ports — For example, deny access to Port 80 (HTTP) for outsiders

   a. Router looks at (1) the packet source IP address and source TCP/UDP port and (2) the destination IP address and destination TCP/UDP port

2. <u>Proxy Server or application gateway</u> — Examines where the is being routed and the type of information in the packet

   a. Difference between proxy and packet filtering is that proxy delivers the packet

   b. Modifies source identification of client packets sent from within organization — This disguises the internal client from the rest of the Internet and acts as a proxy agent for the client on the Internet — Reduces potential for hackers to gain info about internal network — May include logging and authentication features

   c. Slower than packet filtering

3. <u>Circuit level gateway or generic application proxy</u> — Similar to proxy server, but does not need to understand type of info that is being transmitted — Perform Stateful inspection or dynamic packet filtering to make filtering decisions

XV. **Orange Book**

A. DOD Trusted Computer System Evaluation Criteria — Systems classified from A (most trusted) to D (least trusted) — Relates <u>only</u> to standalone systems — NO NETWORKS — Takes a long time to certify (1-2 years) — Based on the Bell-La Padula model — Not adapted to client/server model — Levels:

1. A – Verified Protection — A1

2. B – MAC — B1, B2, and B3

3. C – DAC — C1 and C2.

4. D – Minimal security — Systems evaluated, but failed.

XVI. Red Book

A. Extends Orange Book to networks.

XVII. TCP/IP

A. IP is protocol to transport packets between computers

1. TCP ports data to applications

2. TCP packet uses the IP packet to find which computer it is addressed to

3. Both sending and receiving applications are assigned ports to identify them — Port 80 Web access; SMTP is port 25, FTP is port 21

4. TCP port numbers are divided into three ranges: well-known ports (0-1023), registered ports (1024-49151), and dynamic private ports (49152-65535)

B. IP address is 32 bits — 4 Octets — Address range for each octet is 0-255 — Classes A, B, C, D, and E

XVIII. VPN

A. Internet Protocol Security (IPSec) is accepted standard for VPNs between networks — PPTP (Point to point tunneling protocol), L2F (Layer 2 Forwarding), and L2TP (Layer 2 Tunneling Protocol) are used mostly for remote access, like dial-up — Encryption and authentication — Do not neglect access control

B. Two approaches: DoV (Data over voice) using dial-up or DoD (Data over Data) using Internet access

XIX. Glossary

A. ACL: types of access – read, write, create, execute, modify, delete, rename

B. CERT: Computer Emergency Response Team

C. DNS: Domain Name System — Distributed database of name-to-IP address mappings

D. DNSSEC: secure DNS

E.   Domain: collection of computers and user accounts managed by a central authority

F.   Footprinting: Process by which a hacker gains information about a target computer system

G.   FQDN: Fully Qualified Domain Name — IBM.com

H.   Gap Appliance: Provides "air gap" between trusted and untrusted systems — External CPU, switch, and internal CPU — Internal system never directly connected to the outside

I.   Gateway: translators between networks using incompatible transport protocols

J.   Generic Security Services API (GSSAPI): provides generic authentication, key exchange, and encryption interface for different systems and authentication methods

K.   IETF: When submitted to the IETF, draft docs are valid for six months — They go through a screening process — If draft is accepted, it will be issued as a Request for Comments (RFC) document — If a specification is adopted as an Internet standard, it is given the additional label of STD, but keeps the RFC number

L.   IEEE 802.11 Wireless Standard: wireless LAN standard —Default is transmission in the clear

M.   IKE — Internet Key Exchange protocol

N.   IKMP — Internet Key Management protocol

O.   IPSec: IP security — Two main protocols are Authentication Header (AH) and Encapsulating Security Payload (ESP) — AH provides integrity, authentication, and non-repudiation — ESP provides encryption

P.   LDAP: Lightweight Directory Application Protocol — Can be used to store X.509 certificates for authentication — Subset of X.500 — Simple mechanism for directory clients to query and manage a database of hierarchical entries — LDAP is based on client-server model — LDAP server will offer directory data via TCP/IP port 389 and SSL encrypted port 636 — Primary security concerns are availability and integrity

Q.   Logic Bomb: A logic bomb is a set of instructions in a computer program periodically executed in a computer system that determines conditions or states of the computer, facilitating the perpetration of an unauthorized, malicious act

R.   Message Security Protocol (MSP) — offers confidentiality, authentication, non-repudiation, return receipt, signature

S.   NIC: Network Interface Card

T.   Open View: Leaving confidential documents in public place (on desk)

U.   Public Key Cryptography Standards (PKCS) — provides agreed upon format for Public Key Cryptography; extension to PEM

V.   RADIUS: Remote Authentication Dial-In User Service — Internet standard for remote-access authentication, authorization, and accounting

W.   RPC — Remote Procedure Call — Transport and application layer

X. SAS70 Audit: Statement of Auditing Standards 70

    1. Not a security audit

    2. Only confirms a company's compliance with its own procedures — Those procedures may relate to security

    3. Does not guarantee best practices

    4. Does not make any recommendations for improvement

    5. Prime purpose is to audit controls in place to prevent or detect an error that would be significant to a financial audit

    6. AICPA

Y. SQL: Structured Query Language — standardized language for relational DBMS — schema, tables, views (filtered data)

Z. S/MIME: Secure Multipurpose Internet Mail Extensions — Symmetric key encrypted with public key cryptography — Uses X.509

AA. Secure HTTP (SHTTP): alternative to SSL —S-HTTP can be used to protect individual WWW documents — provides authentication, confidentiality, integrity, and non-repudiation and supports a variety of encryption algorithms

BB. SSH2 Protocol: secure terminal sessions with three components: (1) transport layer protocol, (2) user authentication protocol, (3) connection protocol

CC. SSL: Developed by Netscape — HTTPs

DD. SSO: Single Sign On

EE. Structured Programming: Using programming rules and procedures and preprogrammed modules

FF. Superzap — IBM mainframe utility used to install zaps or fixes to MVS OS or application program code — All powerful — Circumvents all security — Use checksums to detect changes to programs

GG. TEMPEST: TEMPEST certified hardware, rooms, or buildings are shielded to limit EM radiation from computer equipment

HH. TLS: Transaction Layer Security — Confidentiality, authentication and integrity above the transport layer and resides between the application and the TCP layer — SSL and TLS use X.509

II. Wireless Application Protocol (WAP): Used by wireless devices to access the Internet — Uses Wireless Transport Layer Security Protocol (WTLS) — Data must be unencrypted at gateway between wireless and wired network to be re-encrypted using SSL — WTLS provides three classes of security:

    1. Class 1 (Anonymous Authentication) — Neither client or server is authenticated.

    2. Class 2 (Server Authentication)

    3. Class 3 (Two way Client and Server Authentication)

JJ.   Worm: eats up computer/network resources

KK.   WORM: Write Once Read Many

LL.   X.500: Directory protocol — Lookup is based on a unique Distinguished Name (DN) — Each entry in X.500 database associated with a DN will have attributes and values

MM.   X.509: defines mechanism for certificates, supports authentication of entries in an X.500 directory — Features include: Version, Serial Number (unique to certificate, assigned by CA), signature algorithm identifier (identifies algorithm used by CA to sign certificate), Issuer Name (typically the CA), validity period, subject name (DN), public key — International Telecommunication Union (ITU) provides telecom standards, including X —standards — The IETF has recognized X.509 to be used in Internet technologies