NEW CISSP CBK NOTES

V 1.0

September 25, 2015

AMAR NATH

Email:amar.ncet@gmail.com

NOTE: This notes is only a reference and to be used as a supplement to any preparation you already have in place. This note covers CISSP CBK Fourth Edition

Domain 1: Security and Risk Management

Confidentiality

Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis.

Means to achieve: Data Classification, access controls, Encryption

Integrity

Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Means to achieve: Segregation of duties, approval checkpoints in the systems development life cycle (SDLC), implementation of testing practices, Well-formed transactions, need to access

Availability

Availability is the principle that ensures that information is available and accessible to users when needed.

Means to achieve: Up-to-date and active anti-malicious code detection system, tested incident management plans, and disaster recovery planning or business continuity planning

Security Governance

Information security governance provides the mechanisms for the board of directors and management to have the proper oversight to manage the risk to the enterprise to an acceptable level. The intent of governance is to guarantee that the appropriate information security activities are being performed to ensure that the risks are appropriately reduced, the information security investments are appropriately directed, and that executive management has visibility into the program and is asking the appropriate questions to determine the effectiveness of the program.

**Approval of policy must be done at the executive level. Typically standards, procedures, and baselines do not require that level of approval.

**Recommendations for specific controls should be risk based.

Information Security Strategies

Strategic Planning

Strategic plans are aligned with the strategic business and information technology goals. These plans have a longer-term horizon (three to five years or more) to guide the long term view of the security activities.

Tactical Planning

Tactical plans provide the broad initiatives to support and achieve the goals specified in the strategic plan. Tactical plans are shorter in length, such as 6–18 months to achieve a specific security goal of the company.

Operational and Project Planning

Specific plans with milestones, dates, and accountabilities provide the communication and direction to ensure that the individual projects are completed.

The Complete and Effective Security Program

Vision Statement

Vision statements are not technical and focus on the advantages to the business. The vision statement is a high-level set of statements that is brief, to the point, and achievable.

Mission Statement

Mission statements are objectives that support the overall vision. These become the road map to achieving the vision and help the council clearly view the purpose for its involvement.

The vision and mission statements should also be reviewed on an annual basis to ensure that the council is still functioning according to the values expressed in the mission statement, as well as to ensure that new and replacement members are in alignment with the objectives of the council.

Data/Information Custodian/Steward

Data custodian is an individual or function that takes care of the information on behalf of the owner. These individuals ensure that the information is available to the end-users and is backed up to enable recovery in the event of data loss or corruption. This group administers access rights to the information assets on behalf of the information owners.

Due Care

Primarily a legal term used to describe the care a “reasonable person” would exercise under given circumstances. In other words, it is used to also describe what an individual’s or organization’s legal duty is considered to be.

Due Diligence

Due diligence is similar to due care with the exception that it is a preemptive measure made to avoid harm to other persons or their property. If performed correctly, due diligence leads to due care when needed and avoids other situations where due care may need to be exercised.

Due diligence is a practice that should be adopted by the information security professionals as a core tenant of their career.

Governance, Risk Management, and Compliance (GRC)

Governance ensures that the business focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes, and addresses how expected performance will be evaluated. All of this happens within a clearly defined context that might span a division, the entire organization, or a specific set of cross-discipline functions.

Risk management is a systematic process for identifying, analyzing, evaluating, remedying, and monitoring risk. As a result of this process, an organization or group might decide to mitigate a risk, transfer it to another party, or assume the risk along with its potential consequences.

Compliance generally refers to actions that ensure behavior complies with established rules as well as the provision of tools to verify that compliance. It encompasses compliance with laws as well the enterprise's own policies, which in turn can be based on best practices. Compliance requirements are not static, and compliance efforts should not be either.

Intellectual Property Laws

Patent: Patent grants the owner a legally enforceable right to exclude others from practicing the invention covered for a specific time (usually 20 years). A patent is the "strongest form of intellectual property protection."

Trademark: Trademark laws are designed to protect the goodwill an organization invests in its products, services, or image. Trademark law creates exclusive rights to the owner of markings that the public uses to identify various vendor or merchant products or goods.

Copyright: A copyright covers the expression of ideas rather than the ideas themselves; it usually protects artistic property such as writing, recordings, databases, and computer programs.
Trade Secret: A trade secret refers to proprietary business or technical information, processes, designs, practices, etc., that are confidential and critical to the business.

**Wassenaar Arrangement has been established in order to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations.20 Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities that undermine these goals and are not diverted to support such capabilities.
**Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.

Data Breaches

Incident – A security event that compromises the integrity, confidentiality, or availability of an information asset.
Breach – An incident that results in the disclosure or potential exposure of data.
Data Disclosure – A breach for which it was confirmed that data was actually disclosed (not just exposed) to an unauthorized party.

**The Vocabulary for Event Recording and Incident Sharing (VERIS) is designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS Community Database (VCDB) project enlists the cooperation of volunteers in the security community in an attempt to record all publicly disclosed security incidents in a free and open dataset.
**GLBA applies to financial institutions and provides for the implementation of standards to limit the purposeful disclosure of and protect against unauthorized access to consumers' "nonpublic personal information." The GLBA also mandates that a financial institution must provide to its consumers notice of its policies on sharing nonpublic personal information. HIPAA, on the other hand, sets national standards for the security of electronically protected health information. Additionally, HIPAA requires covered entities – i.e., healthcare providers, health plans, and healthcare clearinghouses – and business associates to give notice to consumers whose unsecured protected health information has been compromised due to a breach.

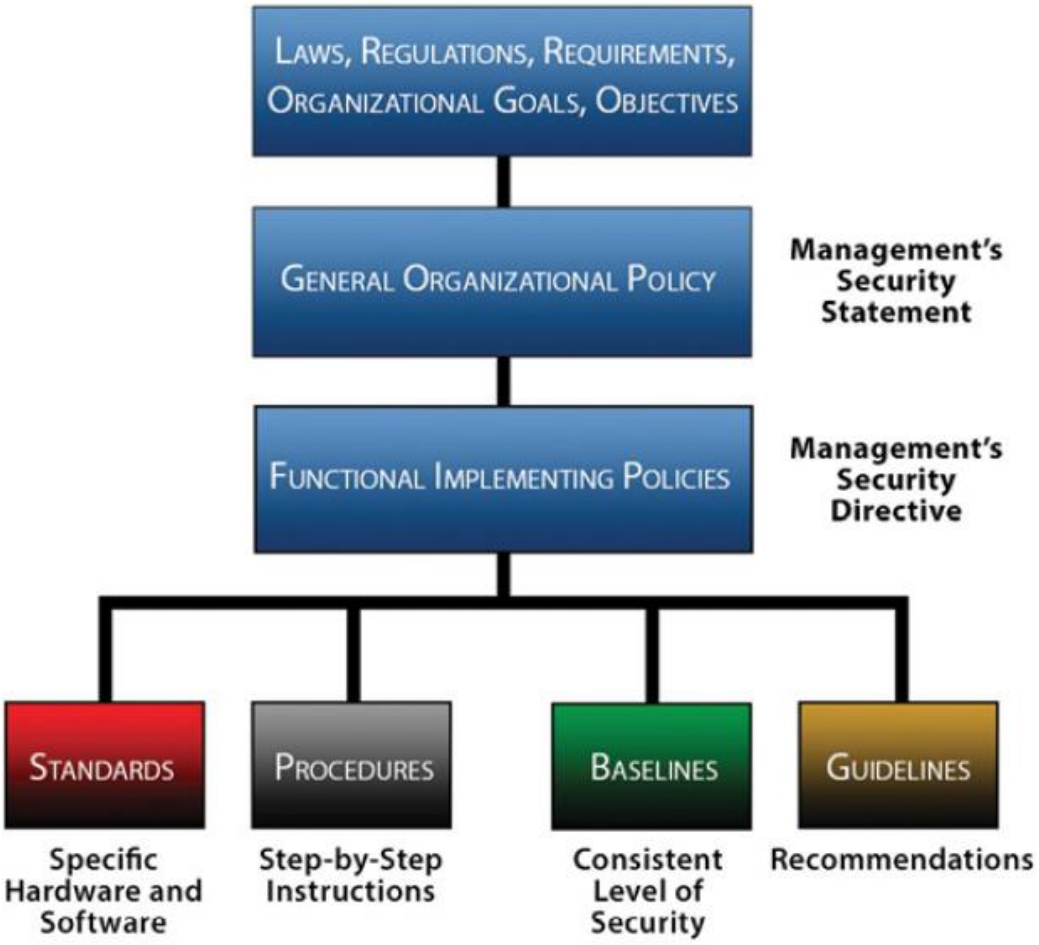
Common Computer Ethics Fallacies

Computer Game Fallacy (users tend to think that computers will generally prevent them from cheating and doing wrong)
Law-Abiding Citizen Fallacy (Computer users often do not realize they also have a responsibility to consider the ramifications of their actions and to behave accordingly.)
Shatterproof Fallacy (Computer users believe that they can do little harm accidentally with a computer beyond perhaps erasing or messing up a file.)
Candy-from-a-Baby Fallacy (Illegal and unethical activity, such as software piracy and plagiarism, are very easy to do with a computer. However, just because it is easy does not mean that it is right.)
Hacker Fallacy (Numerous reports and publications of the commonly accepted hacker belief is that it is acceptable to do anything with a computer as long as the motivation is to learn and not to gain or make a profit from such activities.)
Free Information Fallacy (A somewhat curious opinion of many is the notion that information "wants to be free," as mentioned earlier.)

(ISC)² Code of Professional Ethics

Protect Society, the Commonwealth, and the Infrastructure
Act Honorably, Honestly, Justly, Responsibly, and Legally
Provide Diligent and Competent Service to Principals
Advance and Protect the Profession

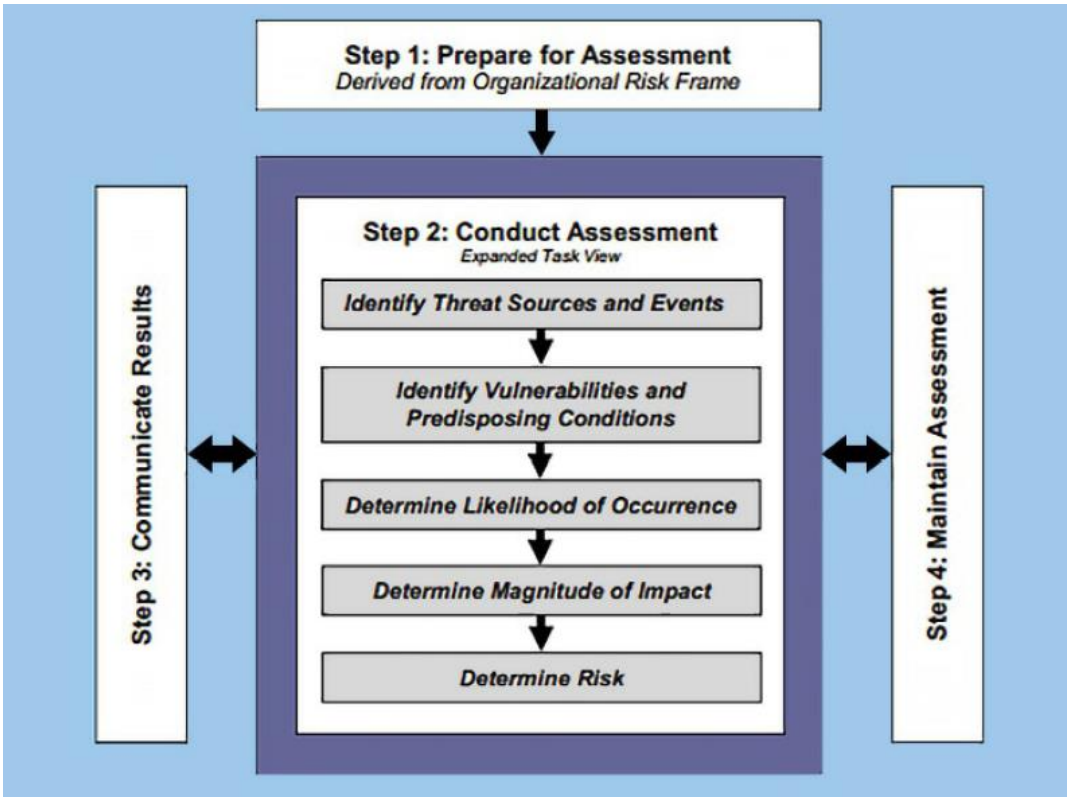
Develop and Implement Security Policy



The risks to the organization are found in three areas:

- Financial
- Reputational
- Regulatory

Risk Management



Prepare for the assessment:
The objective of this step is to establish a context for the risk assessment. This context is established and informed by the results from the risk framing step of the risk management process. Risk framing identifies, for example, organizational information regarding policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, scope of the assessments, rigor of analyses, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the organization.

Conduct the assessment:
The objective of this step is to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. To accomplish this objective, organizations analyze threats and vulnerabilities, impacts and likelihood, and the uncertainty associated with the risk assessment process.

Communicate the assessment results:
The objective of this step is to ensure that decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions.

Maintain the assessment:
The objective of this step is to keep current the specific knowledge of the risk organizations incur.

Risk monitoring provides organizations with the means to, on an ongoing basis, determine the effectiveness of risk responses, identify risk-impacting changes to organizational information systems and the environments in which those systems operate, and verify compliance.
Maintaining risk assessments includes the following specific tasks:

- Monitor risk factors identified in risk assessments on an ongoing basis and understand subsequent changes to those factors; and
- Update the components of risk assessments reflecting the monitoring activities carried out by organizations.

An organization may also wish to document evidence of the countermeasure in a deliverable called an exhibit, or in some frameworks this is called "evidence." An exhibit can be used to provide an audit trail for the organization and, likewise, evidence for any internal or external auditors that may have questions about the organization's current state of risk.

Security and Audit Frameworks and Methodologies

Framework

Committee of Sponsoring Organizations of the Treadway Commission (COSO)
COSO identifies five areas of internal control necessary to meet the financial reporting and disclosure objectives. These include:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and Communication
5. Monitoring

IT Infrastructure Library (ITIL)
Control Objectives for Information and Related Technology (COBIT)
ISO 27002:2013

Risk Assessment Methodologies

NIST SP 800–30r1, 800-39, and 800–66r1
CRAMM (CCTA Risk Analysis and Management Method)
Failure Modes and Effect Analysis
Facilitated Risk Analysis Process (FRAP) - Narrow risk assessment
OCTAVE - People from an organization manage and direct an information security risk evaluation for their organization.
Security Officers Management and Analysis Project (SOMAP) - Ppen information security management project and maintain free and open tools and documentation under the GNU license.
Spanning Tree Analysis
VAR (Value at Risk) - VAR methodology provides a summary of the worst loss due to a security breach over a target horizon. They can achieve the best balance between risk and cost of implementing security controls.

Qualitative Risk Assessments

Risk = Likelihood * Impact

Quantitative Risk Assessments

SLE = Asset Value (in $) × Exposure
ALE = SLE x ARO

Risk Treatment

Risk Avoidance
Risk Transfer
Risk Mitigation
Risk Acceptance

Access Control Categories

1. **Directive** – Controls designed to specify acceptable rules of behavior within an organization
2. **Deterrent** – Controls designed to discourage people from violating security directives
3. **Preventive** – Controls implemented to prevent a security incident or information breach
4. **Compensating** – Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
5. **Detective** – Controls designed to signal a warning when a security control has been breached
6. **Corrective** – Controls implemented to remedy circumstance, mitigate damage, or restore controls
7. **Recovery** – Controls implemented to restore conditions to normal after a security incident.

Access Control Types

Administrative Controls – Sometimes called Management Controls, these are procedures implemented to define the roles, responsibilities, policies, and administrative functions needed to manage the control environment.
Logical (Technical) Controls – These are electronic hardware and software solutions implemented to control access to information and information networks.
Physical Controls – These are controls to protect the organization's people and physical environment, such as locks, fire management, gates, and guards. Physical controls may be called "operational controls" in some contexts.

**tailoring and supplementation may be used by the security professional. Tailoring involves scoping the assessment procedures to more closely match the characteristics of the information system and its environment of operation. The tailoring process gives organizations the flexibility needed to avoid assessment approaches that are unnecessarily complex or costly while simultaneously meeting the assessment requirements established by applying the fundamental concepts in their risk management framework. Supplementation involves adding assessment procedures or assessment details to adequately meet the risk management needs of the organization (e.g., adding organization-specific details such as system/platform-specific

information for selected security controls). Supplementation decisions should be made in consultation with the senior management of the organization in order to maximize flexibility in developing security assessment plans when applying the results of risk assessments in determining the extent, rigor, and level of intensity of the assessments.

Security Assessment

- Vulnerability Assessment
- Control Assessment
- Penetration Testing

Penetration Testing Strategies

- External testing
- Internal testing
- Blind testing
- Double-blind testing
- Targeted testing

Penetration Test Methodology

1. **Reconnaissance/Discovery** – Identify and document information about the target.
2. **Enumeration** – Gain more information with intrusive methods.
3. **Vulnerability Analysis** – Map the environment profile to known vulnerabilities.
4. **Execution** – Attempt to gain user and privileged access.
5. **Document Findings** – Document the results of the test.

Continuous Improvement

The plan-do-check-act (PDCA) cycle, also known as Deming Cycle or Shewhart Cycle:
Plan – Identify an opportunity and plan for change.
Do – Implement the change on a small scale.
Check – Use data to analyze the results of the change and determine whether it made a difference.
Act – If the change was successful, implement it on a wider scale and continuously assess your results. If the change did not work, begin the cycle again.

**Pretexting is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.
**Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. Phone phishing =vishing
**Baiting Attack - the attacker leaves a malware infected CD-ROM or USB flash drive in a location sure to be found.
**The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers. The SLR document evolves into a draft Service Level Agreement.

Domain 2: Asset Security

Quality control (QC) is an assessment of quality based on internal standards, processes, and procedures established to control and monitor quality, while **quality assurance (QA)** is an assessment of quality based on standards external to the process and involves reviewing of the activities and quality control processes to insure final products meet predetermined standards of quality. While quality assurance procedures maintain quality throughout all stages of data development, quality control procedures monitor or evaluate the resulting data products.

Data verification as the process of evaluating the completeness, correctness, and compliance of a dataset with required procedures to ensure that the data is what it purports to be. **Data validation** follows data verification, and it involves evaluating verified data to determine if data quality goals have been achieved and the reasons for any deviations. While data verification checks that the digitized data matches the source data, validation checks that the data makes sense. Data entry and verification can be handled by personnel who are less familiar with the data, but validation requires in-depth knowledge about the data and should be conducted by those most familiar with the data.

Data modeling is the methodology that identifies the path to meet user requirements. The focus should be to keep the overall model and data structure as simple as possible while still adequately addressing project participant's business rules and project goals and objectives.

Data Remanence

Clearing

Clearing is the removal of sensitive data from storage devices in such a way that there is assurance that the data may not be reconstructed using normal system functions or software file/data recovery utilities. The data may still be recoverable but not without special laboratory techniques.

Purging

Purging or sanitizing is the removal of sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique.

Destruction

The storage media is made unusable for conventional equipment. Effectiveness of destroying the media varies. Destruction using appropriate techniques is the most secure method of preventing retrieval.

Overwriting

Degaussing

Encryption

SSDs have a unique set of challenges that require a specialized set of data destruction techniques. Unlike HDDs, overwriting is not effective for SSDs. Because the flash translation layer controls how the system is able to access the data, it can effectively "hide" data from data destruction software, leaving iterations of the data un-erased on different sections of the drive. Instead, SSD manufacturers include built-in sanitization commands that are designed to internally erase the

data on the drive. The benefit of this is that the flash translation layer does not interfere with the erasure process.

Classification is concerned primarily with access, while categorization is primarily concerned with impact.

Compliant Encryption Tools

The various tools to encrypt data can be divided into 3 broad categories: Self-Encrypting USB Drives, Media Encryption Software, and File Encryption Software.

Self-Encrypting USB Drives – Portable USB drives that embed encryption algorithms within the hard drive, thus eliminating the need to install any encryption software. The limitation of such devices is that the files are only encrypted when residing on the encrypted USB drive, which means files copied from the USB drive to be sent over email or other file sharing options will not protected.

Media Encryption Software – Software that is used to encrypt otherwise unprotected storage media such as CDs, DVDs, USB drives, or laptop hard drives. The flexibility of this software allows protection to be applied to a greater selection of storage media. However, the same limitation on collaboration applies to media encryption software as it does to Self-Encrypting USB Drives.

File Encryption Software – Allows greater flexibility in applying encryption to specific file(s). When using File Encryption Software properly, resource owners can share encrypted files over email or other file sharing mechanisms while maintaining protection.

****Scoping** guidance provides an enterprise with specific terms and conditions on the applicability and implementation of individual security controls. **Tailoring** involves scoping the assessment procedures to more closely match the characteristics of the information system and its environment of operation.

Security Content Automation Protocol (SCAP)

SCAP is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. SCAP is a multi-purpose framework of specifications that support automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement. Goals for the development of SCAP include standardizing system security management, promoting interoperability of security products, and fostering the use of standard expressions of security content.

Domain 3: Security Engineering

A **multitasking** system switches from one process to another quickly to speed up processing. Another way to achieve higher performance can be realized by increasing the number of processors in a system where each processor can assume some of the load. Powerful computers such as servers have several processors handling different tasks, although there must be one processor to control the flow of instructions and data through the supplementary processors. This type of system is called a **multiprocessing** system. **Multithreading**, then, is the concept whereby the OS time slices the threads and gives one thread some time on the CPU, then switches to another thread and lets it run for a while.

Memory Protection

The three most common ones are segmentation, paging, and protection keying. **Segmentation** refers to dividing a computer's memory into segments. A reference to a memory location includes a value that identifies a segment and an offset within that segment. **Paging** divides the memory address space into equal-sized blocks called pages. A page table maps virtual memory to physical memory. Page tables make it easier to allocate additional memory, as each new page can be allocated from anywhere in physical memory. It is impossible for an application to access a page that has not been explicitly allocated to it because every memory address either points to a page allocated to that application or generates an interrupt called a page fault. Unallocated pages, and pages allocated to any other application, do not have any addresses from the application point of view. A **protection key** mechanism divides physical memory up into blocks of a particular size, each of which has an associated numerical value called a protection key. Each process also has a protection key value associated with it. When memory is accessed, the hardware checks that the current process's protection key matches the value associated with the memory block being accessed; if not, then an exception occurs.

ASLR involves randomly arranging the positions of key data areas of a program, including the base of the executable and the positions of the stack, heap, and libraries in a process's memory address space. Address space layout randomization is based upon the low chance of an attacker guessing the locations of randomly placed areas. Security is increased by increasing the search space. **Executable space protection** is the marking of memory regions as non-executable, implying that any attempt to execute machine code in these regions will cause an exception.

Enterprise Security Architecture

Rather than focus on individual functional and nonfunctional components in an individual application, it focuses on a strategic design for a set of security services that can be leveraged by multiple applications, systems, or business processes. ESA is focused on setting the long-term strategy for security services in the enterprise. Its primary purpose is to establish the priorities for security services development and provide that input into information security program

planning. It focuses on the design and implementation of common security services and the enforcement of security zones of control.

A **security zone of control** is an area or grouping within which a defined set of security policies and measures are applied to achieve a specific level of security. Zones are used to group together those entities with similar security requirements and levels of risk and ensure each zone is adequately segregated from another zone.

Common Architecture Frameworks

Zachman Framework - not specific to security architecture
Sherwood Applied Business Security Architecture (SABSA) Framework - chain of traceability
The Open Group Architecture Framework (TOGAF) - architecture development method (ADM), architecture content framework (ACF)
IT Infrastructure Library (ITIL) – service strategy, service design, service transition, service operations, and continuous service improvement

Types of Security Models

State Machine Model - Once the system is determined to be in a secure state, the state machine model will ensure that every time the system is accessed, it will be accessed only in accordance with the security policy rules. This process will guarantee that the system will transition only from one secure state to another secure state.
Multilevel Lattice Models - A multilevel security model describes strict layers of subjects and objects and defines clear rules that allow or disallow interactions between them based on the layers they are in. According to this type of model, the clearance of the subject is compared with the classification of the data to determine access.
Noninterference Models - Type of multilevel model with a high degree of strictness, severely limiting any higher-classified information from being shared with lower-privileged subjects even when higher-privileged subjects are using the system at the same time. They also deal with the effects of covert channels that may leak information inappropriately.
Matrix-Based Models - Matrix-based models focus on one-to-one relationships between subjects and objects. Ex access control matrix.
Information Flow Models - Information flow models focus on how information is allowed or not allowed between individual objects.

Examples of Security Models

Subjects -> Clearances || Objects -> Classification

Bell–LaPadula (Confidentiality Model) - lattice-based model
Simple security property – No read up
* property – No Write down
Strong * property – All interaction at same level
No integrity, No need to know, No one-to-one mapping

Biba (Integrity Model) - lattice-based model
Simple security property – No read down
* property – No Write up
Invocation property – No service request to object at higher level

Clark–Wilson (Integrity Model)
Transactions by authorized subjects be evaluated by another party before they were committed on the model system - Separation of duties (External Consistency)
Strict definition of well-formed transactions. Clark–Wilson establishes a system of subject–program–object bindings such that the subject no longer has direct access to the object. (Internal Consistency)

Lipner Model
Lipner combines elements of Bell–LaPadula and Biba together. First to separate objects into data and programs.

Brewer–Nash (The Chinese Wall) Model
This model focuses on preventing conflict of interest when a given subject has access to objects with sensitive information associated with two competing parties.

Graham–Denning Model
Graham–Denning is primarily concerned with how subjects and objects are created, how subjects are assigned rights or privileges, and how ownership of objects is managed. In other words, it is primarily concerned with how a model system controls subjects and objects at a very basic level where other models simply assumed such control.

**Functional Requirements – address what the design must do or accomplish.
This includes what types of controls need to be included, what assets must be protected, what common threats must be addressed, and what vulnerabilities have been found. In other words, functional requirements will guide what security services will be included in the design.
**Nonfunctional Requirements – focus on the qualities of the services, including any requirements for reliability and performance.

Information Systems Security Evaluation Models

Certification - The product or system is tested to see whether it meets the documented requirements (including any security requirements).
Accreditation - Management evaluates the capacity of a system to meet the needs of the organization.
Protection profile Description of a needed security solution.
Target of evaluation Product proposed to provide a needed security solution.
Security target Vendor's written explanation of the security functionality and assurance mechanisms that meet the needed security solution—in other words, "This is what our product does and how it does it."

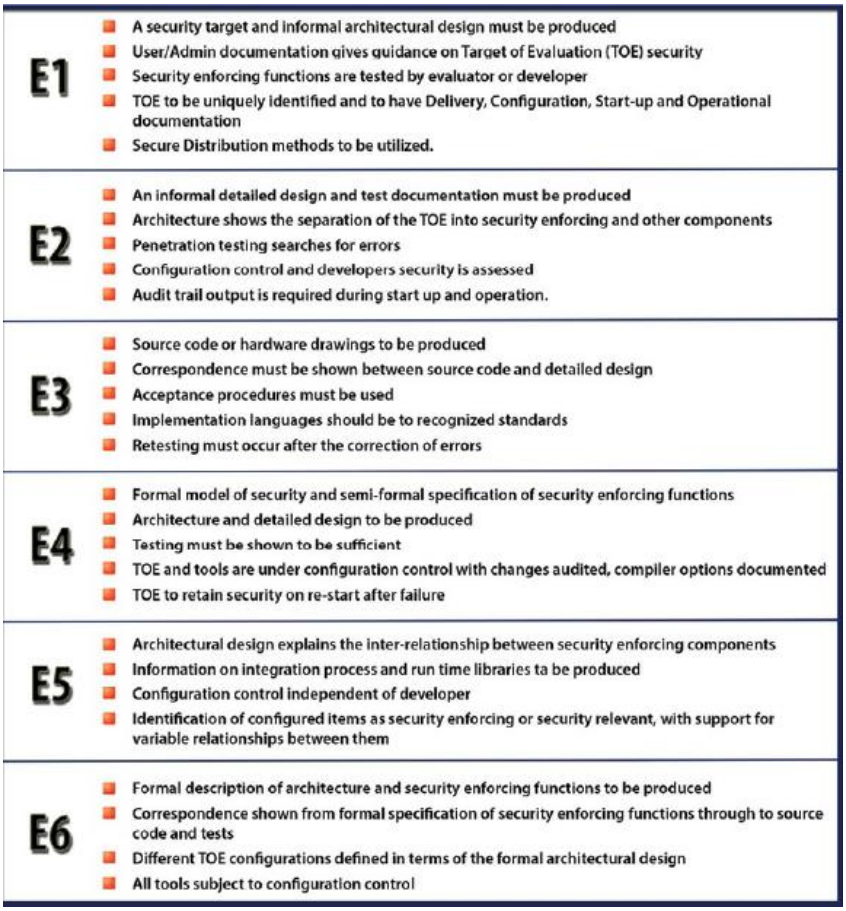
Security functional requirements Individual security functions which must be provided by a product.
Security assurance requirements Measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.
Packages—EALs Functional and assurance requirements are bundled into packages for reuse. This component describes what must be met to achieve specific EAL ratings.

Product Evaluation Models (TCSEC, ITSEC, CC)

Trusted Computer System Evaluation Criteria (TCSEC) – Orange Book
Addressed Only Confidentiality, TCB, Very specific and rigid

Evaluation Division	*Evaluation Class*	*Degree of Trust*
A - Verified Protection	***A1*** - Verified Design	Highest
B - Mandatory Protection	***B3*** - Security Domains ***B2*** - Structured Protection ***B1*** - Labeled Security Protection	
C - Discretionary Protection	***C2*** - Controlled Access Protection ***C1*** - Discretionary Security Protection	
D - Minimal Protection	***D1*** - Minimal Protection	Lowest

Information Technology Security Evaluation Criteria (ITSEC)
Included integrity and availability, ST, TOE, Assignment of assurance



Common Criteria

Protection Profiles: Common set of functional and assurance requirements for a category of vendor products deployed in a particular type of environment.

- **EAL1** Functionally tested
- **EAL2** Structurally tested
- **EAL3** Methodically tested and checked
- **EAL4** Methodically designed, tested, and reviewed
- **EAL5** Semiformally designed and tested
- **EAL6** Semiformally verified design and tested
- **EAL7** Formally verified design and tested

Industry and International Security Implementation Guidelines

ISO/IEC 27001 and 27002 Security Standards

1. **Information Security Policies** – Provide management guidance and support for information security.

2. **Organization of Information Security** – Provides a formal and defined security mechanism within an organization that includes information processing facilities and information assets accessed or maintained by third parties.

3. **Human Resource Security** – Provides security aspects for employees joining, moving, and leaving an organization.
4. **Asset Management** – Protects the organization's assets by ensuring valuable data assets are identified and receive appropriate protection.
5. **Access Control** – Limits access to data, mobile communications, telecommunications, and network services, as well as detects unauthorized activities.
6. **Cryptography** – Provides the ability to protect the confidentiality, integrity, and authenticity of information.
7. **Physical and Environmental Security** – Prevents unauthorized physical access, damage, and interference to facilities and data.
8. **Operations Security** – Ensures the proper and secure operation of data processing facilities by protecting software, communications, data, and the supporting infrastructure.
9. **Communications Security** – Ensures proper data exchange between organizations.
10. **Information Systems Acquisitions, Development, and Maintenance** – Implements security controls into operations and development systems to ensure the security of application system's software and data.
11. **Supplier Relationships** – Implements security controls to protect corporate information and assets that are accessible by suppliers and ensure that suppliers provide the agreed upon level of service and security.
12. **Information Security Incident Management** – Implements procedures to detect and respond to information security incidents.
13. **Information Security Aspects of Business Continuity Management** – Mitigates an incident's impact on critical business systems.
14. **Compliance** – Ensures adherence to criminal and civil laws and statutory, regulatory, or contractual obligations, complies with organizational security policies and standards, and provides for a comprehensive audit process.

An organization's ISMS may be certified by a licensed third-party assessor under ISO/IEC 27001:2013, but their control practices cannot be.

Control Objects for Information and Related Technology (COBIT)
COBIT provides a set of generally accepted processes to assist in maximizing the benefits derived using information technology (IT) and developing appropriate IT governance.
Payment Card Industry Data Security Standard (PCI-DSS)
PCI- DSS provides the security architect with a framework of specifications to ensure the safe processing, storing, and transmission of cardholder information. PCI-DSS is focused on compliance with the standard that includes prevention, detection, and reaction to security incidents.

Security Capabilities of Information Systems

**When no subject can gain access to any object without authorization, this is referred to as complete mediation. Complete mediation is normally the responsibility of the security kernel implementing the reference monitor concept.

**Supervisor state -> Kernel mode, Problem state -> User mode
****Emanations:** System emanations are unintentional electrical, mechanical, optical, or acoustical energy signals that contain information or metadata about the information being processed, stored, or transmitted in a system. TEMPEST is a set of standards designed to shield buildings and equipment to protect them against eavesdropping and passive emanations gathering attempts.
**State attacks are also known as "race conditions," which attempt to take advantage of how a system handles multiple requests.
****Covert channels** are communications mechanisms hidden from the access control and standard monitoring systems of an information system. TCSEC identifies two types of covert channels:

Storage channels that communicate via a stored object
Timing channels that modify the timing of events relative to each other.

The only way to mitigate covert channels is through the secure design of an information system.
****Data marts** are smaller versions of data warehouses. While a data warehouse is meant to contain all of an organization's information, a data mart may contain the information from just a division or only about a specific topic.
****Inference** is the ability to deduce (infer) sensitive or restricted information from observing available information.
****Aggregation** is combining non-sensitive data from separate sources to create sensitive information.
****Grid computing** is the sharing of CPU and other resources across a network in such a manner that all machines function as one large computer. Grid computers are often used for processor intensive tasks, which are suitable to be processed by parallel tasks. Grid computing is often confused with "cluster computing." Both involve using two or more computers to solve problems, but grid computing is heterogeneous while cluster computing is homogenous. Grid computers can have different operating systems, hardware, and software. Grid systems are also associated with multi-tasking (a desktop computer may be part of a grid with spare CPU resources and also serve normal desktop functions), whereas a cluster is devoted to a single task. Finally, clusters are most often physically close together with a fast bus or network connecting the nodes, while a grid is geographically dispersed.

Private Cloud – The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community Cloud – The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

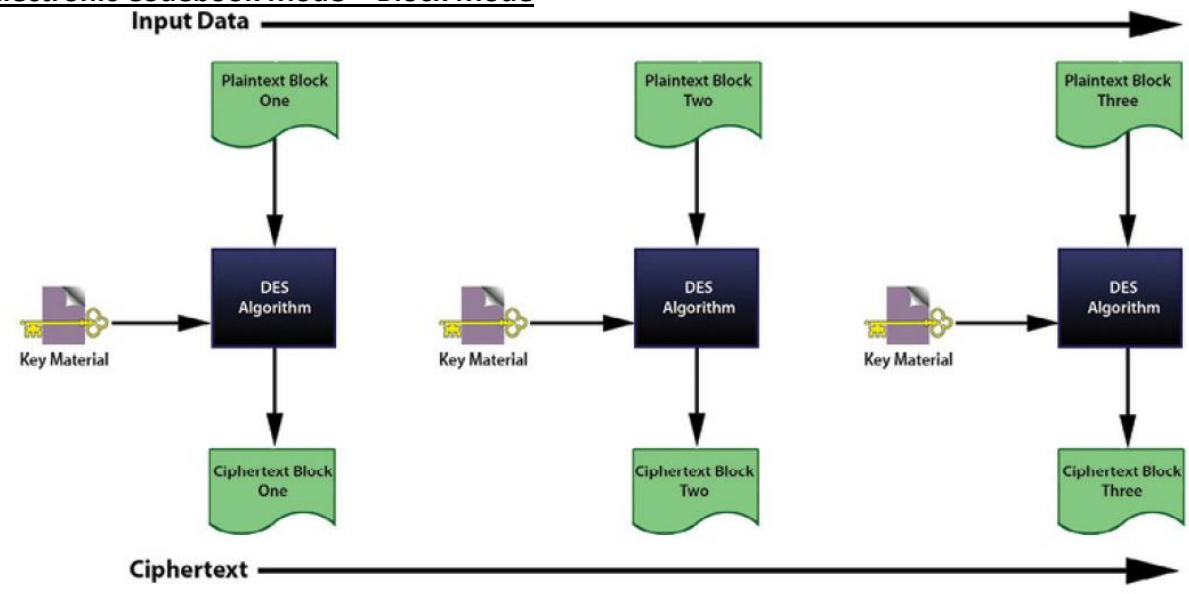
Public Cloud – The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid Cloud – The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Cryptographic Systems

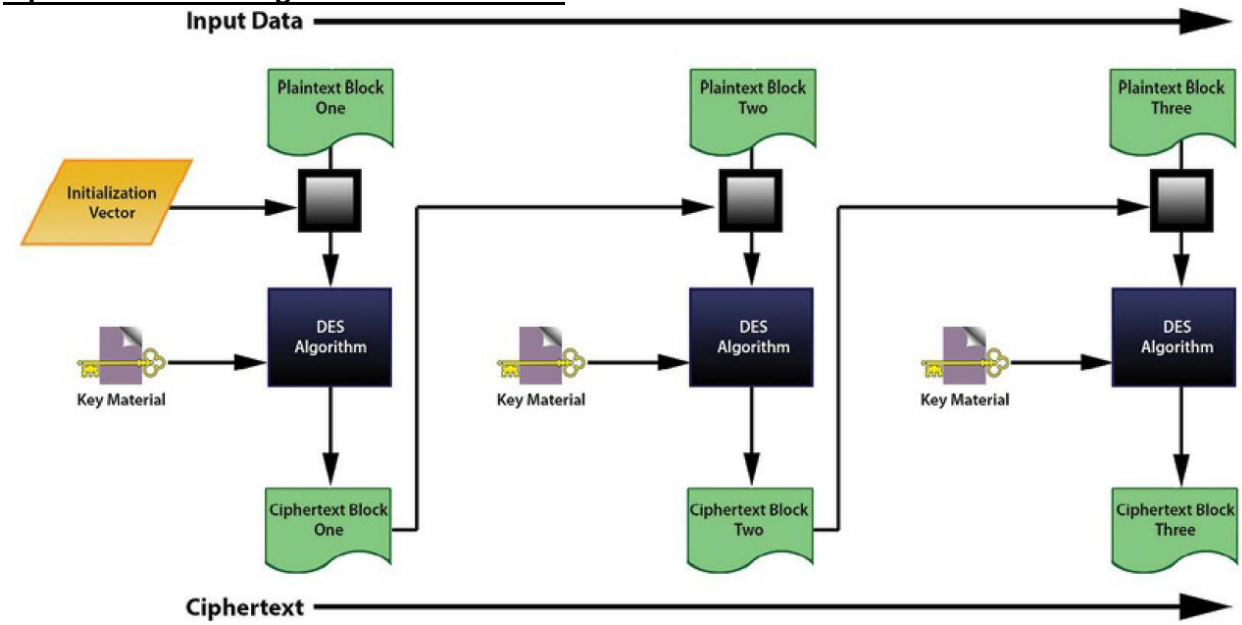
**Key Clustering – When different encryption keys generate the same ciphertext from the same plaintext message.
**Confusion is provided by mixing (changing) the key values used during the repeated rounds of encryption. When the key is modified for each round, it provides added complexity that the attacker would encounter.
**Diffusion is provided by mixing up the location of the plaintext throughout the ciphertext. Through transposition, the location of the first character of the plaintext may change several times during the encryption process, and this makes the cryptanalysis process much more difficult.

Data Encryption Standard (DES)

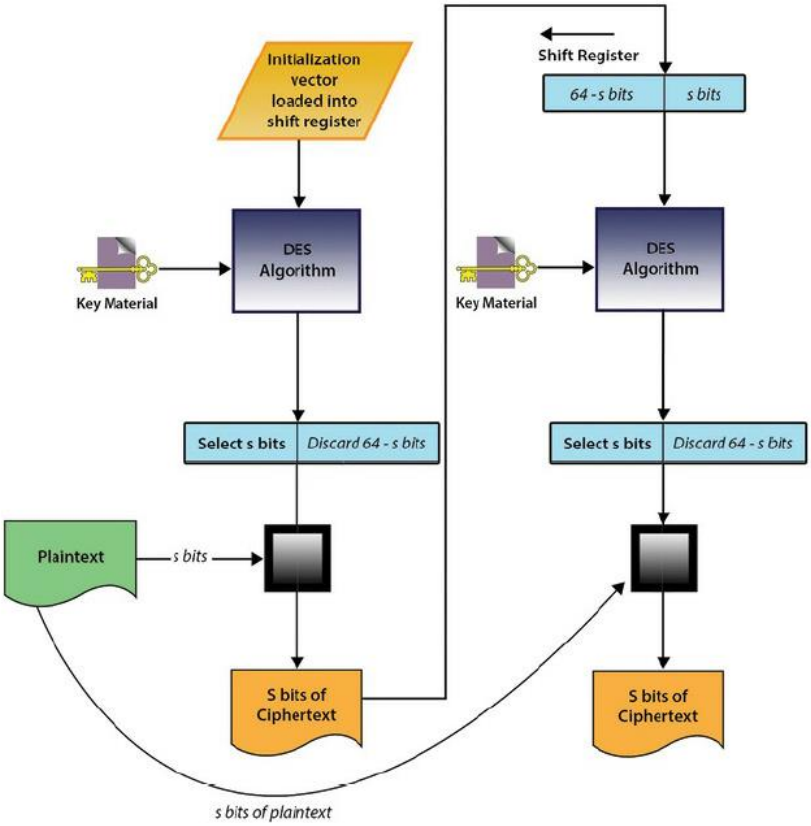
64 Bit block – 56 Bit Key
Modes:
Electronic Codebook Mode – Block Mode



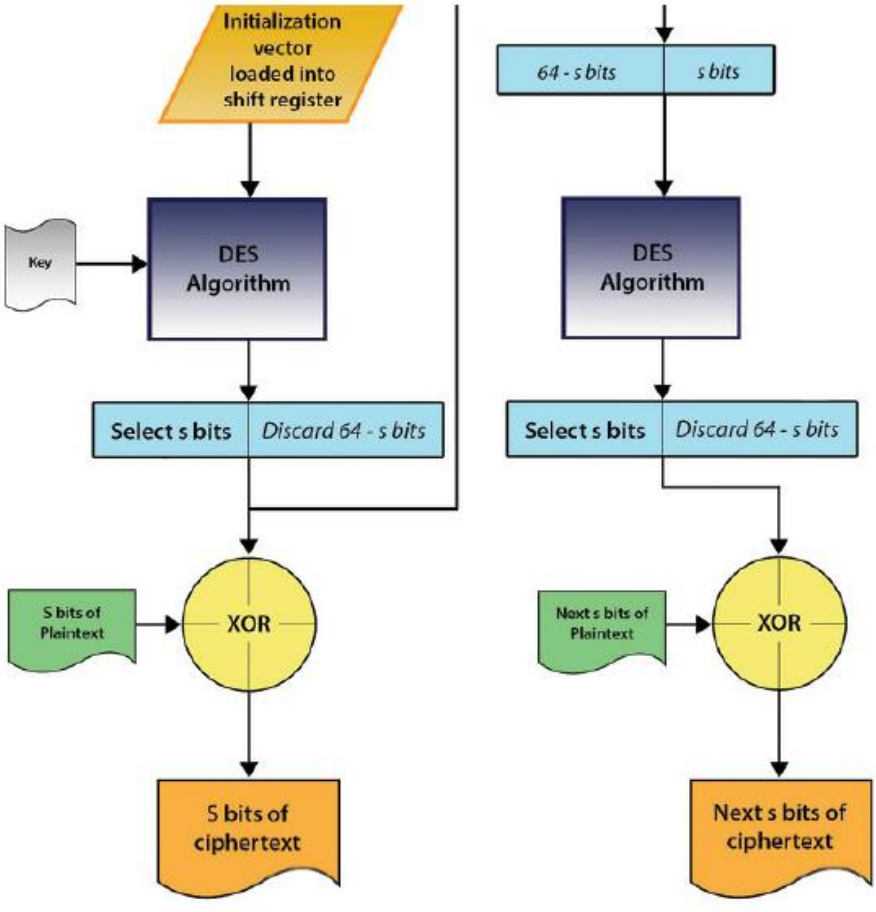
Cipher Block Chaining Mode – Block Mode



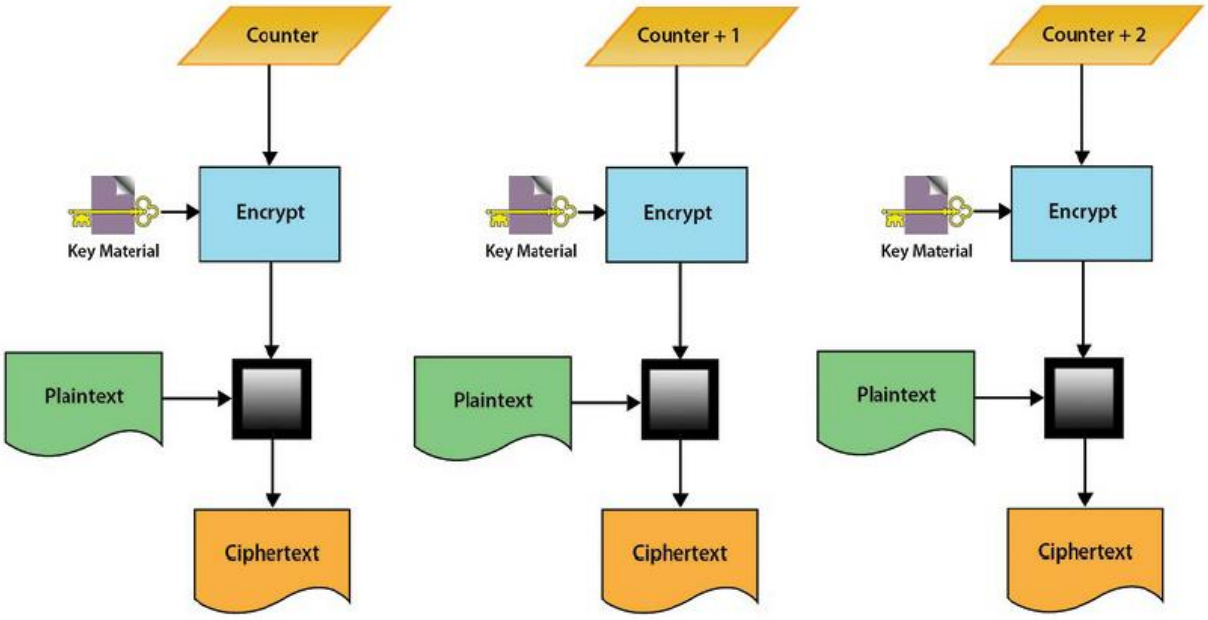
Cipher Feedback Mode – Stream Mode



Output Feedback Mode – Stream Mode



Counter Mode – Stream Mode



**** DES is susceptible to a brute force attack & Meet in the Middle**

Advanced Encryption Standard

Rijndael beat out the other finalists: Serpent, MARS, RC6 & TwoFish.

The Rijndael operation consists of four major operations.

1. Substitute Bytes – Use of an S-box to do a byte-by-byte substitution of the entire block.
2. Shift Rows – Transposition or permutation through offsetting each row in the table.
3. Mix Columns – A substitution of each value in a column based on a function of the values of the data in the column.
4. Add Round Key – XOR each byte with the key for that round; the key is modified for each round of operation.

Symmetric Algorithms

- Data Encryption Standard (DES)
- 3DES (Triple DES)
- Blowfish
- Twofish
- International Data Encryption Algorithm (IDEA)
- RC4, RC5, and RC6
- Advanced Encryption Standard (AES)
- Secure and Fast Encryption Routine (SAFER)
- Serpent
- CAST

Asymmetric Algorithms

- RSA – factoring the product of two large prime numbers
- Diffie–Hellmann Algorithm – mathematical function based first on finding the primitive root of a prime number
- El Gamal – discrete logs
- Elliptic Curve Cryptography (ECC) - ECC implementations provides savings on computational power and bandwidth

SAML - The Security Assertion Markup Language is an XML-based standard used to exchange authentication and authorization information.

Cyber Physical Systems (CPS) are smart networked systems with embedded sensors, processors, and actuators that are designed to sense and interact with the physical world (including the human users) and support real-time, guaranteed performance in safety critical applications.

** PKI – Certificates – X.509

**XML Key Management Specification 2.0 (XKMS) - The two parts of the XML Key Management Specification 2.0 are the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS). First, X-KISS describes a syntax that allows a client (i.e., application) to delegate part or all of the tasks required to process XML Signature < ds:KeyInfo > elements to a Trust service. Secondly, X-KRSS describes a protocol for registration of public key information. The key material can be generated by the X-KRSS, on request to support easier key recovery, or manually.

ANSI X9.17 was developed to address the need of financial institutions to transmit securities and funds securely using an electronic medium. Specifically, it describes the means to ensure the secrecy of keys.

**Split knowledge focuses on the uniqueness of separate objects that must be joined together. Dual control has to do with forcing the collusion of at least two or more persons to combine their split knowledge to gain access to an asset. Both split knowledge and dual control complement each other and are necessary functions that implement the segregation of duties in high integrity cryptographic environments.
(Dual control – 2 or more subjects, Split knowledge – 2 or more objects)

**Key encrypting key (KEK). KEKs are used as part of key distribution or key exchange. The process of using a KEK to protect session keys is called key wrapping.

Digital Signatures
It is a block of data (a pattern of bits, usually a hash) that is generated based on the contents of the message sent and encrypted with the sender's private key.

Hashing
MD5 Message Digest Algorithm – 128 bit digest from 512 bit block
SHA – 160 bit digest
HAVAL
RIPEMD-160
**Birthday attacks possible

Methods of Cryptanalytic Attacks

Ciphertext-Only Attack (Only Cipheretext)
Known Plaintext (Both Plaintext and Ciphertext available)
Chosen Plaintext (Known algorithm, Adaptive where Plaintext can be changed)
Chosen Ciphertext (Known algorithm, Adaptive where Ciphertext can be changed)

Asymmetric cryptosystems are vulnerable to chosen ciphertext attacks.

**Differential Cryptanalysis, Also called a side channel attack, this more complex attack is executed by measuring the exact execution times and power required by the crypto device to perform the encryption or decryption.

Side-Channel Attacks are passive attacks that rely on a physical attribute of the implementation such as power consumption/emanation. These attributes are studied to determine the secret key and the algorithm function. Some examples of popular side channels include timing analysis and electromagnetic differential analysis.
Fault Analysis attempts to force the system into an error state to gain erroneous results. By forcing an error, gaining the results, and comparing it with known good results, an attacker may learn about the secret key and the algorithm.
Probing Attacks attempt to watch the circuitry surrounding the cryptographic module in hopes that the complementary components will disclose information about the key or the algorithm. Additionally new hardware may be added to the cryptographic module to observe and inject information.
Replay Attack, This attack is meant to disrupt and damage processing by the attacker, through the resending of repeated files to the host. If there are no checks such as time-stamping, use of one time tokens, or sequence verification codes in the receiving software, the system might process duplicate files.

Physical security

Crime Prevention through Environmental Design (CPTED)

Crime Prevention through Environmental Design (CPTED) is a crime reduction technique that has several key elements applicable to the analysis of the building function and site design against physical attack. It is used by architects, city planners, landscapers, interior designers, and security professionals with the objective of creating a climate of safety in a community by designing a physical environment that positively influences human behavior.

Types of Glass

Tempered Glass

Tempered glass is similar to the glass installed in car windshields. It will resist breakage and will disintegrate into small cubes of crystals with no sharp edges. Tempered glass is used in entrance doors and adjacent panels.

Wired Glass

Wired glass provides resistance to impact from blunt objects. The wire mesh is imbedded into the glass thereby providing limited protection.

Laminated Glass

Laminated glass is recommended for installation in street-level windows, doorways, and other access areas. It is made from two sheets of ordinary glass bonded to a middle layer of resilient plastic. When it is struck, it may crack but the pieces of glass tend to stick to the plastic inner material.

Bullet Resistant (BR) Glass

Bullet resistant glass is typically installed in banks and high-risk areas. There are different layers of BR glass with the standard being 1 ¼-inch thick, which provides protection from a 9mm round.

Glass Break Sensors - Acoustic sensors listen for an acoustic sound wave that matches the frequency of broken glass - shock sensors feel the shock wave when glass is broken - dual-technology glass break sensors – both acoustic and shock wave – is most effective.

Garages - Lighting levels of at least 10 to 12 foot-candles over parked cars and 15 to 20 foot-candles in walking and driving aisles is recommended - exterior lights should be placed approximately 12 feet above ground.

Fire extinguishers

Class A – Extinguishers are for ordinary combustible materials such as paper, wood, cardboard, and most plastics.

Class B – Fires involve flammable or combustible liquids such as gasoline, kerosene, grease, and oil.

Class C – Fires involve electrical equipment, such as appliances, wiring, circuit breakers, and outlets. Never use water to extinguish class C fires – the risk of electrical shock is far too great.

Class D – Fire extinguishers are commonly found in a chemical laboratory. They are for fires that involve combustible metals, such as magnesium, titanium, potassium, and sodium.

Fire Suppression

Wet Systems – Have a constant supply of water in them at all times; once activated, these sprinklers will not shut off until the water source is shut off.

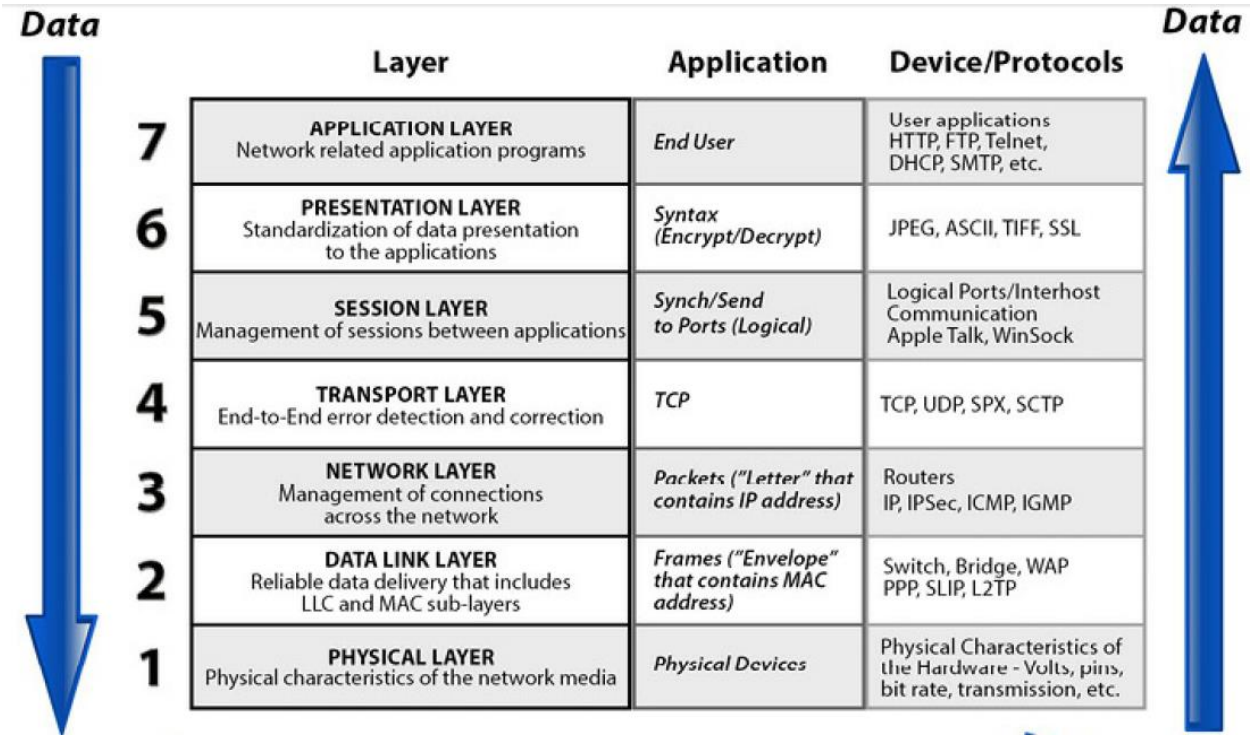
Dry Systems– Do not have water in them. The valve will not release until the electric valve is stimulated by excess heat.

Pre-Action Systems – Incorporate a detection system, which can eliminate concerns of water damage due to false activations. Water is held back until detectors in the area are activated.

Deluge Systems – Operate in the same function as the pre-action system except all sprinkler heads are in the open position.

Aero-K, FM-200 -> Fire suppression in server room, Safe for occupied places.

Domain 4: Communication & Network Security



	Layer	Application	Device/Protocols
7	**APPLICATION LAYER** Network related application programs	*End User*	User applications HTTP, FTP, Telnet, DHCP, SMTP, etc.
6	**PRESENTATION LAYER** Standardization of data presentation to the applications	*Syntax (Encrypt/Decrypt)*	JPEG, ASCII, TIFF, SSL
5	**SESSION LAYER** Management of sessions between applications	*Synch/Send to Ports (Logical)*	Logical Ports/Interhost Communication Apple Talk, WinSock
4	**TRANSPORT LAYER** End-to-End error detection and correction	*TCP*	TCP, UDP, SPX, SCTP
3	**NETWORK LAYER** Management of connections across the network	*Packets ("Letter" that contains IP address)*	Routers IP, IPSec, ICMP, IGMP
2	**DATA LINK LAYER** Reliable data delivery that includes LLC and MAC sub-layers	*Frames ("Envelope" that contains MAC address)*	Switch, Bridge, WAP PPP, SLIP, L2TP
1	**PHYSICAL LAYER** Physical characteristics of the network media	*Physical Devices*	Physical Characteristics of the Hardware - Volts, pins, bit rate, transmission, etc.

Layer 1: Physical Layer

Physical topologies are defined at this layer.

Layer 2: Data Link Layer

The data link layer prepares the packet that it receives from the network layer to be transmitted as frames on the network. This layer ensures that the information that it exchanges with its peers is error free.

Logical Link Control (LLC) – Manages connections between two peers. It provides error and flow control and control bit sequencing.
Media Access Control (MAC) – Transmits and receives frames between peers. Logical topologies and hardware addresses are defined at this sublayer. An Ethernet's 48-bit hardware address is often called a MAC address as a reference to the name of the sublayer.

Layer 3: Network Layer

The network layer moves information between two hosts that are not physically connected.
Internet Protocol (IP) – Addressing, Fragmentation, connectionless protocol

***Routing Protocol used to exchange routing information between devices. Not actual packets.*

Routing Information Protocol (RIP)

Standard for exchange of routing information among gateways and hosts, interior gateway protocol, distance vector

Open Shortest Path First (OSPF)

Interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm.

Internet Control Message Protocol (ICMP)

1. ICMP Error Messages
2. ICMP Query Messages

Announce Network Errors, Announce Network Congestion, Assist Troubleshooting, Announce Timeouts

Internet Group Management Protocol (IGMP)

IGMP is used to manage multicasting groups, which are a set of hosts anywhere on a network that are interested in a particular multicast. Multicast agents administer multicast groups, and hosts send IGMP messages to local agents to join and leave groups.

Layer 4: Transport Layer

TCP, UDP
TCP three way handshake
1. First, the client sends a SYN segment. This is a request to the server to synchronize the sequence numbers. It specifies its initial sequence number (ISN), which is incremented by 1, and that is sent to the server. To initialize a connection, the client and server must synchronize each other's sequence numbers.

2. Second, the server sends an ACK and a SYN in order to acknowledge the request of the client for synchronization. At the same time, the server is also sending its request to the client for synchronization of its sequence numbers. There is one major difference in this transmission from the first one. The server transmits an acknowledgement number to the client. The

acknowledgement is just proof to the client that the ACK is specific to the SYN the client initiated. The process of acknowledging the client's request allows the server to increment the client's sequence number by one and uses it as its acknowledgement number.

3. Third, the client sends an ACK in order to acknowledge the request from the server for synchronization. The client uses the same algorithm the server implemented in providing an acknowledgement number. The client's acknowledgment of the server's request for synchronization completes the process of establishing a reliable connection.

Layer 5: Session Layer

This layer provides a logical, persistent connection between peer hosts.

Layer 6: Presentation Layer

Data conversion
Character code translation
Compression
Encryption and decryption
Presentation layer can be composed of two sublayers:
Common application service element (CASE) and Specific application service element (SASE)

Layer 7: Application Layer

Application's portal to network-based services

Border Gateway Protocol (BGP)

BGP is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems. BGP is often the protocol used between gateway hosts on the Internet.

**An extranet differs from a DMZ (demilitarized network zone) in the following way: An extranet is made available to authenticated connections that have been granted an access account to the resources in the extranet. Conversely, a DMZ will host publicly available resources that must support unauthenticated connections from just about any source, such as DNS servers and email servers.

**A router may send an ICMP redirect to a host to tell it to use a different, more effective default route. However, an attacker can send an ICMP redirect to a host telling it to use the attacker's machine as a default route. The attacker will forward all of the redirected traffic to a router so that the victim will not know that his or her traffic has been intercepted. This is a good example of a man-in-the-middle attack.

DNS – TCP/53, UDP/53
LDAP – TCP/389, UDP/389, X.500
NetBIOS – TCP/137,138, UDP/135,139

CIFS/SMB – TCP/445, Samba(Unix)
SMTP – TCP/25, ESMTP
FTP – TCP(20-DATA, 21-CONTROL)

- Secure FTP with TLS (Encrypted FTP)
- SFTP (SSH FTP – Not a FTP but SSH used for file transfer)
- FTP over SSH (Tunnel FTP traffic over SSH)

Active mode (PORT mode) – Sever initiates the data connection
Passive mode (PASV mode) – Client initiates the data connection

TFTP – UPD/69

SCADA
Control Server – A control server hosts the software and often the interfaces used to control actuators, coils, and PLCs through subordinate control modules across the network.

Remote Terminal Unit (RTU) – The RTU supports SCADA remote stations often equipped with wireless radio interfaces and is used in situations where land based communications may not be possible.

Human-Machine Interface (HMI) – The HMI is the interface where the humans (operators) can monitor, control, and command the controllers in the system.

Programmable Logic Controller (PLC) – The PLC is a small computer that controls relays, switches, coils, counters, and other devices.

Intelligent Electronic Devices (IED) – The IED is a sensor that can acquire data and also provide feedback to the process through actuation. These devices allow for automatic control at the local level.

Input/Output (IO) Server – The IO server is responsible for collecting process information from components such as IEDs, RTUs, and PLCs. They are often used to interface third-party control components such as custom dashboards with a control server.

Data Historian – The data historian is like the Security Event and Incident Management (SEIM) for industrial control systems. It is typically a centralized database for logging process information from a variety of devices.

Converged Protocols

Fibre Channel over Ethernet (FCoE) - FCoE is a lightweight encapsulation protocol and lacks the reliable data transport of the TCP layer. FCoE is only for short-haul communication within a data center. Data Center Bridging (DCB) merges this to Ethernet. Most for SAN.

Internet Small Computer System Interface (iSCSI) - iSCSI is Internet SCSI (Small Computer System Interface), an Internet Protocol (IP)-based storage networking standard for linking data storage facilities. By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. Because of the ubiquity of IP networks, iSCSI can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet and can enable location-independent data storage and retrieval. Two objective - Storage Consolidation, Disaster Recovery.

Multi-Protocol Label Switching (MPLS) - Layer 2.5 networking protocol, MPLS does "label switching" instead. The first device does a routing lookup, just like before, but instead of finding a next-hop, it finds the final destination router. And it finds a pre-determined path from "here" to that final router. The router applies a "label" (or "shim") based on this information. Future routers use the label to route the traffic without needing to perform any additional IP lookups. At the final destination router, the label is removed, and the packet is delivered via normal IP routing.

Label Switched Path (LSP)
MPLS Router Roles/Positions are:

Label Edge Router (LER) or "Ingress Node" – The router that first encapsulates a packet inside an MPLS LSP. Also the router that makes the initial path selection.

Label Switching Router (LSR) or "Transit Node" – A router that only does MPLS switching in the middle of an LSP.

Egress Node – The final router at the end of an LSP, which removes the label.

P/PE/CE

P – Provider Router – A core/backbone router that is doing label switching only. A pure P router can operate without any customer/Internet routes at all. This is common in large service provider networks.

PE – Provider Edge Router – A customer facing router that does label popping and imposition.

CE – Customer Edge – The customer device a PE router talks to.

Two main MPLS routing protocols:

Label Distribution Protocol (LDP) – No Traffic engineering

Resource Reservation Protocol with Traffic Engineering (RSVP-TE) – Supports traffic engineering

MPLS Pseudowires - Layer 2 Pseudowire or VLL (Virtual Leased Line) is an emulated layer-2 point-to-point circuit, delivered over MPLS. They can be used to interconnect two different types of media such as Ethernet to Frame Relay. Difficult to load balance.

MPLS L3VPNs - An L3VPN is an IP based VPN. Networks build virtual routing domains (VRFs) on their edge routers. Customers are placed within a VRF and exchange routes with the provider router in a protected routing-instance, usually BGP or IGP. They can support complex topologies and interconnect many sites. They are usually load-balancing hash friendly because they have exposed IP headers.
MPLS VPLS - VPLS (Virtual Private LAN Service) creates an Ethernet multipoint switching service over MPLS. It is used to link a large number of customer endpoints in a common broadcast domain.
MPLS Fast Reroute - MPLS Fast Reroute improves convergence during a failure by pre-calculating backup paths for potential link or node failures. With MPLS Fast Reroute, the next best path calculation happens before the failure actually occurs.

**Packet Loss Concealment (PLC) is used in VoIP communications to mask the effect of dropped packets. Zero substitution, Waveform substitution.
**Jitter - It does not occur because of the packet delay, but because of a variation of packet delays.

Types of Certificates

- Client SSL certificates
- Server SSL certificates
- S/MIME certificates
- Object-Signing certificates
- Certificate Authority (CA) certificates

Online Certificate Status Protocol - OCSP is used for obtaining the revocation status of an X.509 digital certificate. Vulnerable to replay attacks.

**Bastion Host – A data diode only allows information to flow in a single direction; for instance, it enforces rules that allow information to be read, but nothing may be written.
**Bridges do no filter broadcasts.
**Circuit-Level Proxy – Only forwards packets. No inspection
**Application-Level Proxy - Web proxy. Inspects packets. AUP can enforce.

VPN

IPSec – Suite of protocols.
Authentication Header (AH) provides data integrity, data origin authentication, and protection from replay attacks.
Encapsulating Security Payload (ESP) provides confidentiality, data-origin authentication, and data integrity.

Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for security association creation and key exchange.
Internet Key Exchange (IKE) provides authenticated keying material for use with ISAKMP.

Transport Mode and Tunnel Mode
End points communicate with IPSec using either transport or tunnel mode. In transport mode, the IP payload is protected. This mode is mostly used for end-to-end protection, for example, between client and server. In tunnel mode, the IP payload and its IP header are protected. The entire protected IP packet becomes a payload of a new IP packet and header. Tunnel mode is often used between networks, such as with firewall-to-firewall VPNs.

Internet Key Exchange (IKE)
Internet key exchange allows communicating partners to prove their identity to each other and establish a secure communication channel, and it is applied as an authentication component of IPSec. IKE uses two phases:
Phase 1 – In this phase, the partners authenticate with each other
Phase 2 – The peers' security associations are established, using the secure tunnel and temporary SA created at the end of phase 1.
**A HAIPE (High Assurance Internet Protocol Encryptor) is a Type 1 encryption device that is based on IPSec with additional restrictions, enhancements, and capabilities. A HAIPE is typically a secure gateway that allows two enclaves to exchange data over an untrusted or lower-classification network. Since this technology works at the network layer, secure end-to-end connectivity can take place in heterogeneous environments. This technology has largely replaced link layer encryption technology implementations.

Tunneling

Layer 2 Tunneling Protocol (L2TP)
Point-to-Point Tunneling Protocol (PPTP):
- Works in a client/server model
- Extends and protects PPP connections
- Works at the data link layer
- Transmits over IP networks only

Layer 2 Tunneling Protocol (L2TP):
- Hybrid of L2F and PPTP
- Extends and protects PPP connections
- Works at the data link layer
- Transmits over multiple types of networks, not just IP
- Combined with IPSec for security

IPSec:
- Handles multiple VPN connections at the same time
- Provides secure authentication and encryption
- Supports only IP networks
- Focuses on LAN-to-LAN communication rather than user-to-user

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

Secure Sockets Layer (SSL):

- Works at the transport layer and protects mainly web-based traffic
- Granular access control and configuration are available
- Easy deployment since SSL is already embedded into web browsers
- Can only protect a small number of protocol types, thus is not an infrastructure-level VPN solution

Remote Authentication Dial-in User Service (RADIUS**) - RADIUS is an authentication protocol used mainly in networked environments, such as ISPs, or for similar services requiring single sign-on for layer 3 network access, for scalable authentication combined with an acceptable degree of security.
****SNMP** architecture consists of a management server (called the manager in SNMP terminology) and a client, usually installed on network devices such as routers and switches called an agent. SNMP allows the manager to retrieve "get" values of variables from the agent, as well as "set" variables. The most easily exploited SNMP vulnerability is a brute force attack on default or easily guessable SNMP passwords known as "community strings" often used to manage a remote device.

****Screen Scraper** - A screen scraper is a program that can extract data from output on a display intended for a human.

****Circuit-Switched** Networks - Circuit-switched networks establish a dedicated circuit between end points. These circuits consist of dedicated switch connections. POTS, ISDN, PPP
****Packet-Switched** Networks - Packet-switched networks do not use a dedicated connection between end points. Instead, data is divided into packets and transmitted on a shared network. Each packet contains meta-information so that it can be independently routed on the network.

Attacks on VLAN
MAC Flooding Attack
802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack
Double-Encapsulated 802.1Q/Nested VLAN Attack
ARP Attacks
Multicast Brute Force Attack
Spanning-Tree Attack
Random Frame Stress Attack

Software Defined Networking

Infrastructure Layer ("**Data** Plane") – Network switches and routers and the data itself as well as the process of forwarding data to the appropriate destination.
Control Layer ("**Control** Plane") – The intelligence in devices that works in true "middle-man" fashion, determining how traffic should flow based on the status of the infrastructure layer and the requirements specified by the application layer.

Application Layer ("**Application** Plane") – Network services, utilities, and applications that interface with the control level to specify needs and requirements.
The goal of SDN is to offload the handling of traffic and the way it meets the needs of the applications involved.
**SDS

Network Attacks

FIN SCAN - a request to close a connection is sent to the target machine.
NULL SCAN – No flags are set on the initiating TCP packet
XMAS SCAN - All TCP flags are set
Teardrop - IP packet fragments are constructed so that the target host calculates a negative fragment length when it attempts to reconstruct the packet.
Overlapping Fragment Attack - Overlapping fragment attacks are used to subvert packet filters that only inspect the first fragment of a fragmented packet.
Source Routing Exploitation - IP allows the sender to explicitly specify the path. Could allow an external attacker access to an internal network.
Smurf and Fraggle Attacks - Smurf attack, the intruder sends an ICMP echo request with a spoofed source address of the victim. Fraggle attack uses UDP

NFS Attacks - Export of parts of the file system that were not intended for publication, Using an unauthorized client, Incorrect mapping of user IDs between server and client, Sniffing and access request spoofing, SetUID files
SYN Flooding - A SYN flood attack is a denial-of-service attack against the initial handshake in a TCP connection. Many new connections from faked, random IP addresses are opened in short order, overloading the target's connection table. [Secure network stack]

"Pharming" is the manipulation of DNS records

Domain 5: Identity and Access Management

Identification is the assertion of a unique identity for a person or system.
Authentication is the process of verifying the identity of the user.
Authorization is the process of defining the specific resources a user needs and determining the type of access to those resources the user may have.

- Identification provides uniqueness
- Authentication provides validity
- Authorization provides control

Essential security **characteristics regarding identities: uniqueness, nondescriptiveness, and secure issuance.
SID:S-1-0
Name: Null Authority

SID: S-1-0-0
Name: Nobody
SID: S-1-1
Name: World Authority
Description: An identifier authority.
SID: S-1-1-0
Name: Everyone
Description: A group that includes all users, even anonymous users and guests. Membership is controlled by the operating system.
SID: S-1-5-21domain-500
Name: Administrator
Description: A user account for the system administrator. By default, it is the only user account that is given full control over the system.
SID: S-1-5-21domain-501
Name: Guest
Description: A user account for people who do not have individual accounts. This user account does not require a password. By default, the Guest account is disabled.
SID: S-1-5-21domain-502
Name: KRBTGT
Description: A service account that is used by the Key Distribution Center (KDC) service.
SID: S-1-5-21domain-512
Name: Domain Admins

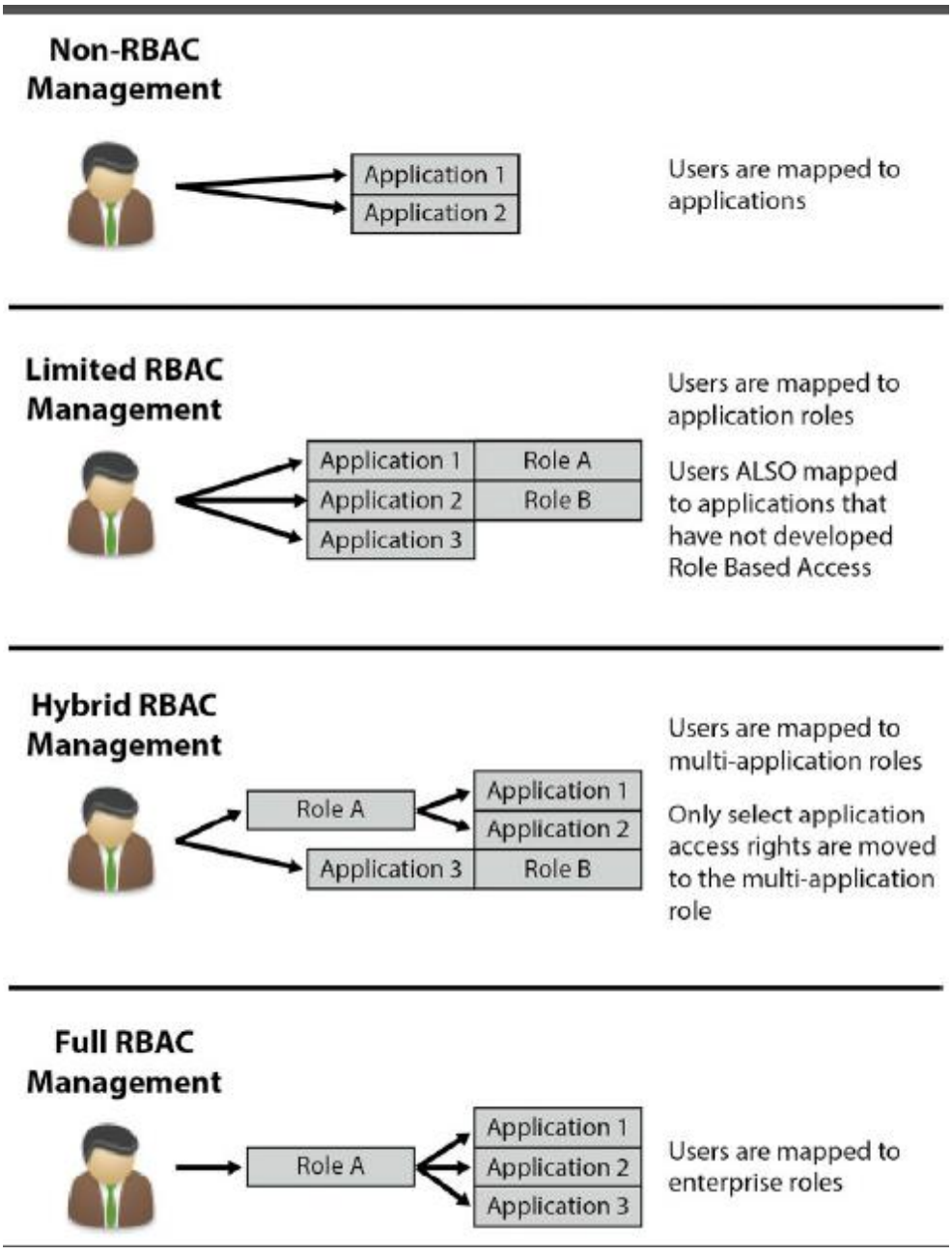
Directory Technologies
X.500
LDAP
Active Directory Domain Services (ADDS)
X.400 - Message Handling Systems (MHS)

KERBEROS:
Authentication protocol for authentication, authorization, and auditing using symmetric encryption.
3 players – The principal, server and KDC (authentication server (AS) and ticket-granting server (TGS))
While acting as the AS, it will authenticate a principal via a pre-exchanged secret key. Once a principal is authenticated, the KDC operates as a TGS, providing a ticket—a piece of electronic data validated by the TGS—to the principal to establish trusted relationships between principals on the network.
"Kerberizing" an application, allows the application to attach to the Kerberos environment, exchange encryption keys and tickets, and communicate securely with other Kerberos-enabled devices and services.

Federated Identity Management - cross-certification model, bridge model.

Authorization Mechanisms

Role-Based Access Control



Non-RBAC – No roles defined
Limited RBAC – Roles defined specific to applications. Direct app access available.
Hybrid RBAC – Roles defined at organizational level. Roles specific to app available.
Fully RBAC – Only org level roles used for access.

Rule-Based Access Control

Access is based on a list of predefined rules that determine what accesses should be granted.

Mandatory Access Controls (MACs)
Mandatory Access Control requires the system itself to manage access controls in accordance with the organization's security policies. Based on Object classification and subjects clearance.

Discretionary Access Controls (DACs)
Controls are placed on data by the owner of the data.

Identity and Access Provisioning Lifecycle – Provisioning, Review, Revocation

Domain 6: Security Assessment and Testing

Real User Monitoring (RUM) is an approach to Web monitoring that aims to capture and analyze every transaction of every user of a website or application. Also known as real user measurement, real-user metrics, or end-user experience monitoring (EUM), it's a form of passive monitoring, relying on Web-monitoring services that continuously observe a system in action, tracking availability, functionality, and responsiveness.
Synthetic performance monitoring, sometimes called proactive monitoring, involves having external agents run scripted transactions against a Web application. These scripts are meant to follow the steps a typical user might use. Useful in alerting and better in assessing site availability & network problems. Synthetic have full control over the client, the detail that can be garnered is impressive. Website Monitoring, Database Monitoring, TCP Port Monitoring.

Code Review and Testing
During Planning and Design - Architecture Security Reviews, Threat Modeling
During Application Development - Static Source Code Analysis (SAST) and Manual Code Review, Static Binary Code Analysis and Manual Binary Review
Executable in a Test Environment - Manual or Automated Penetration Testing, Automated Vulnerability Scanners, Fuzz Testing Tools

Code-based testing is also known as **structural testing** or "**white-box" testing**. It identifies test cases based on knowledge obtained from the source code, detailed design specification, and other development documents. These test cases challenge the control decisions made by the program and the program's data structures including configuration tables. Structural testing can identify "dead" code that is never executed when the program is run. Structural testing is accomplished primarily with unit (module) level testing, but it can be extended to other levels of software testing.
Coverage - Measure of completeness with respect to test selection criteria.

Definition-based or **specification-based testing** is also known as **functional testing** or "**black-box" testing**. It identifies test cases based on the definition of what the software product (whether it be a unit (module) or a complete program) is intended to do. These test cases challenge the intended use or functionality of a program and the program's internal and external

interfaces. Functional testing can be applied at all levels of software testing, from unit to system level testing.

Cause-effect graphing is one functional software testing technique that systematically identifies combinations of inputs to a software product for inclusion in test cases.

Statistical testing, can be employed to provide further assurance that a software product is dependable. Statistical testing uses randomly generated test data from defined distributions based on an operational profile. Statistical testing also provides high structural coverage. It does require a stable software product. Thus, structural and functional testing are prerequisites for statistical testing of a software product.

Regression analysis and testing are employed to provide assurance that a change has not created problems elsewhere in the software product.

Changes made to correct errors and faults in the software are corrective maintenance. Changes made to the software to improve the performance, maintainability, or other attributes of the software system are perfective maintenance. Software changes to make the software system usable in a changed environment are adaptive maintenance.

Negative testing ensures that your application can gracefully handle invalid input or unexpected user behavior. The purpose of negative testing is to detect such situations and prevent applications from crashing. In addition, negative testing helps to improve the quality of the application and find its weak points. A core difference exists between positive testing and negative testing: Throwing an exception is expected in negative testing. When you perform negative testing, exceptions are expected – they indicate that the application handles improper user behavior correctly.

Interface testing is different from integration testing in that interface testing is done to check that the different components of the application or system being developed are in sync with each other or not. In technical terms, interface testing helps determine that different functions like data transfer between the different elements in the system are happening according to the way they were designed to happen. Interface testing is conducted to evaluate whether systems or components pass data and control correctly to one another.

Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. A robust ISCM program thus enables organizations to move from compliance-driven risk management to data-driven risk management providing organizations with information necessary to support risk response decisions, security status information, and ongoing insight into security control effectiveness. An ISCM program helps to ensure that deployed security controls continue to be effective and that operations remain within stated organizational risk tolerances in light of the inevitable changes that occur over time.
NIST 800-137

Audits:
Statement on Auditing Standards (SAS) 70 - SAS 70 was intended to focus specifically on risks related to internal control over financial reporting (ICOFR) and not broader objectives such as system availability and security.
Service Organization Control (SOC) - Addressing security, privacy, and availability concerns.
12 month period
Point in time reports covering design – Type 1
Period of time reports covering design and operating effectiveness – Type 2
SOC 1 – Same as SSAE 16 or SAS 70 which was intended to focus specifically on risks related to internal control over financial reporting *(ICOFR)*
SOC 2 & SOC 3 - *security, availability*, confidentiality, processing integrity, and privacy
SOC 3 - Need to communicate a level of assurance to a broad base of users without having to disclose detailed controls and test results.

Domain 7: Security Operations

Investigations

International Organization of Computer Evidence (IOCE)
Scientific Working Group on Digital Evidence (SWGDE)
Association of Chief Police Officers (ACPO)
NIST SP 800-86: Computer Forensic Guidelines
IACIS forensic examination procedures
ACPO Good Practices Guide for Computer Based Evidence

Locard's exchange principle states that when a crime is committed, the perpetrators leave something behind and take something with them, hence the exchange.

Incident Handling and Response - triage, investigation, containment, and analysis and tracking
Triage encompasses the detection, identification, and notification sub-phases.
Investigative Phase deals directly with the analysis, interpretation, reaction, and recovery from an incident.
Rules of evidence:

- Be authentic
- Be accurate
- Be complete
- Be convincing
- Be admissible

**Classification is concerned primarily with access, while categorization is primarily concerned with impact. Categorization is the process of determining the impact of the loss of confidentiality, integrity, or availability of the information to an organization. 800-60

The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as **coercivity**. It is important to make sure that the coercivity of the degausser is of sufficient strength to meet object reuse requirements when erasing data. If a degausser is used with insufficient coercivity, then a remanence of the data will exist.

The **Spamhaus Project** is an international nonprofit organization whose mission is to track the Internet's spam operations and sources, to provide dependable real time anti-spam protection for Internet networks, to work with law enforcement agencies to identify and pursue spam and malware gangs worldwide, and to lobby governments for effective antispam legislation. Spamhaus maintains a number of security intelligence databases and real time spam-blocking databases ('DNSBLs') responsible for keeping back the vast majority of spam and malware sent out on the Internet. These include the Spamhaus Block List (SBL), the Exploits Block List (XBL), the Policy Block List (PBL), and the Domain Block List (DBL).

BCP DR

Incremental backups take copies of only the files that have changed since the last full or incremental backup was taken and then set the archive bit to "0." An incremental backup takes the most time in restoration because the full backup must be performed first and then every incremental backup taken since the last full backup. More time.
A **differential** backup copies only the files that have had their data change since the last full backup and does not change the archive bit value. More space.

SAN consists of dedicated block level storage on a dedicated network. They can be made of numerous storage devices such as tape libraries, optical drives, and disk arrays. They utilize protocols like iSCSI to appear to operating systems as locally attached devices.
NAS operates at the file level instead of the block level. A NAS is generally designed to simply store and serve files.

Redundant array of independent disk (RAID)
RAID 0 – Stripping**,** Writes files in stripes across multiple disks without the use of parity information.
RAID 1 – Mirroring, duplicates all disk writes from one disk to another to create two identical drives.
RAID 2 – Not used, Data is spread across multiple disks at the bit level using this technique. Redundancy information is computed using a Hamming error correction code, which is the same technique used within hard drives and error- correcting memory modules.
RAID 3 and 4 - Parity information is written to a dedicated 3rd disk. If one of the data disks fails, then the information on the parity disk may be used to reconstruct the drive. Data is striped across multiple disks at the byte level for RAID 3 and at the block level for RAID 4.

RAID 5 - Data and parity information is striped together across all drives. This level is the most popular and can tolerate the loss of any one drive because the parity information on the other drives can be used to reconstruct the lost one.
RAID 6 - This level extends the capabilities of RAID 5 by computing two sets of parity information. The dual parity distribution accommodates the failure of two drives.
RAID 0+1 and RAID 1+0

Database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.
Electronic vaulting is accomplished by backing up system data over a network. Changes to the host system are sent to the vault server in real time when the backup method is implemented as a mirror.
Journaling is a technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location.

Tabletop Exercise/Structured Walk-Through Test
A tabletop exercise/structured walk-through test is considered a preliminary step in the overall testing process and may be used as an effective training tool; however, it is not a preferred testing method. Its primary objective is to ensure that critical personnel from all areas are familiar with the BCP and that the plan accurately reflects the organization's ability to recover from a disaster.
Walk-Through Drill/Simulation Test
A walk-through drill/simulation test is somewhat more involved than a tabletop exercise/structured walk-through test because the participants choose a specific event scenario and apply the BCP to it.
Functional Drill/Parallel Test
Functional drill/parallel testing is the first type of test that involves the actual mobilization of personnel to other sites in an attempt to establish communications and perform actual recovery processing as set forth in the BCP. The goal is to determine whether critical systems can be recovered at the alternate processing site and if employees can actually deploy the procedures defined in the BCP.
Full-Interruption/Full-Scale Test
Full-interruption/full-scale test is the most comprehensive type of test. In a full-scale test, a real life emergency is simulated as closely as possible. Therefore, comprehensive planning should be a prerequisite to this type of test to ensure that business operations are not negatively affected.

Time Domain Reflectometry (TDR) systems send induced radio frequency (RF) signals down a cable that is attached to the fence fabric. Intruders climbing or flexing a fence create a signal path flaw that can be converted to an alarm signal. When the conductor cable is bent or flexed, a part of the signal returns to the origination point. This reflected signal can be converted to an intrusion point by computing the time it takes for the signal to travel to the intrusion point and return.
Lighting
Lighting should enable security personnel and employees to notice individuals at night at a distance of 75 feet or more and to identify a human face at about 33 feet.

Continuous lighting is the most common security lighting system. It consists of a series of fixed lights arranged to flood a given area continuously during darkness with overlapping cones of light.
Standby lighting has a layout similar to continuous lighting; however, the lights are not continuously lit but are either automatically or manually turned on when suspicious activity is detected or suspected by the security personnel or alarm systems.
Movable lighting consists of manually operated, movable searchlights that may be lit during hours of darkness or only as needed. The system normally is used to supplement continuous or standby lighting.
Emergency lighting is a backup power system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative.

Fluorescent lights are highly efficient and cost effective. However, they are temperature sensitive and while improving are not considered an effective outdoor lighting system. This light is better suited inside buildings and facilities.
Mercury vapor lights are the preferred security light that disperses a strong white-bluish cast. They have an extended lamp life; however the downside is they take an amount of time to full light when activated – typical to the lights at a stadium.
Sodium vapor lights provide a soft yellow light and is more efficient than mercury vapor. This light is used in areas where fog can be a problem.
Quartz lamps emit a very bright white light and comes on immediately. They typically provide high wattage from 1500 to 2000 and can be used on perimeters and troublesome areas where high visibility and a daylight scene is required.

Infrared Illuminators – allows night surveillance without the need for additional artificial lighting.

Focal length less – Wide coverage
"*Light-to-dark*" ratio refers to the light intensity (as measured in footcandles or LUX) of the lightest (most reflective surface) to the darkest (least reflective surface). A proper light-to-dark ratio for good CCTV picture clarity is 4:1. The maximum ratio is 8:1.

Balanced Magnetic Switch (BMS) - This device uses a magnetic field or mechanical contact to determine if an alarm signal is initiated. One magnet will be attached to the door and the other to the frame; when the door is opened, the field is broken. A BMS differs from standard magnetic status switches in that a BMS incorporates two aligned magnets with an associated reed switch. If an external magnet is applied to the switch area, it upsets the balanced magnetic field such that an alarm signal is received. Balanced magnetic switches are not susceptible to external magnetic fields and will generate an alarm if tampering occurs.

Passive Infrared (PIR) Sensors - A PIR picks up heat signatures (infrared emissions) from intruders by comparing infrared receptions to typical background infrared levels. A PIR is a motion detector and will not activate for a person who is standing still because the electronics package attached to the sensor is looking for a fairly rapid change in the amount of infrared energy it is seeing.

Vaults
Class M – One quarter hour
Class 1 – One half hour
Class 2 – One hour
Class 3 – Two hours

Domain 8: Security in SDLC

Certification and Accreditation (Security Authorization)
Certification is the process of evaluating the security stance of the software or system against a predetermined set of security standards or policies. Certification also examines how well the system performs its intended functional requirements.
Management, after reviewing the certification, authorizes the software or system to be implemented in a production status, in a specific environment, for a specific period.

ISO/IEC 90003:2004 - application of ISO to Software

Integrated Product Team (DevOps)
Integrated Product and Process Development (IPPD) is a management technique that simultaneously integrates all essential acquisition activities through the use of multidisciplinary teams to optimize the design, manufacturing, and supportability processes. IPPD facilitates meeting cost and performance objectives from product concept through production, including field support. One of the key IPPD tenets is multidisciplinary teamwork through Integrated Product Teams (IPTs).

- Develop and test against production-like systems
- Deploy with repeatable, reliable processes
- Monitor and validate operational quality
- Amplify feedback loops

Software development methods:
Non-Iterative
Waterfall – Structured, Heavy overhead in planning and administration, Good for security
Structured Programming Development – Formal and process oriented, largely taught.
Spiral Method - Sort of nested version of the waterfall method, based on the common Deming PDCA
Cleanroom - Development of high-quality software, goal is to write the code correctly the first time rather than trying to find the problems once they are there. Quality is achieved through design rather than testing and remediation.

Iterative
Prototyping - Build a simplified version (prototype) of the application, release it for review, and use the feedback from the users' review to build a second, better version.

Modified Prototype Model (MPM) - A form of prototyping that is ideal for web application development. It allows for the basic functionality of a desired system or component to be formally deployed in a quick time frame.
Rapid Application Development (RAD) - A form of rapid prototyping that requires strict time limits on each phase and relies on tools that enable quick development.
Joint Analysis Development (JAD) - Originally invented to enhance the development of large mainframe systems. JAD facilitation techniques bring together a team of users, expert systems developers, and technical experts throughout the development life cycle.
Exploratory Model - Assumptions are made as to how the system might work, and further insights and suggestions are combined to create a usable system.

Other models
Computer-Aided Software Engineering (CASE) - The technique of using computers and computer utilities to help with the systematic analysis, design, development, implementation, and maintenance of software.
Component-Based Development - The process of using standardized building blocks to assemble, rather than develop, an application.
Reuse Model - In this model, an application is built from existing components.
Extreme Programming - This is a discipline of software development that is based on values of simplicity, communication, and feedback. Good for small teams.

Database

Any key that could be a primary key is called a candidate key. The primary key is an attribute or set of attributes that uniquely identifies a specific instance of an entity.
Concurrency occurs when the DBMS interleaves actions (reads/writes of database objects) of various transactions.
Atomicity implies executing all its actions in one step or not executing any actions at all.
In the **entity** integrity model, the tuple must have a unique and non-null value in the primary key.
The **referential** integrity model states that for any foreign key value, the referenced relation must have a tuple with the same value for its primary key.
SQL actually consists of three sublanguages. The *data definition language (DDL)* is used to create databases, tables, views, and indices (keys) specifying the links between tables. *Data manipulation language (DML),* used to query and extract data, insert new records, delete old records, and update existing records. System and database administrators utilize *data control language (DCL)* to control access to data. It provides the security aspects of SQL and is therefore our primary area of concern. Some of the DCL commands are:

- COMMIT – Saves work that has been done
- SAVEPOINT – Identifies a location in a transaction to which you can later roll back, if necessary
- ROLLBACK – Restores the database to its state at the last COMMIT
- SET TRANSACTION – Changes transaction options such as what rollback segment to use.

Object-Oriented Database Model - The OO objects are a collection of public and private data items and the set of operations that can be executed on the data.

Online Analytical Processing (OLAP) - OLAP technologies provide an analyst with the ability to formulate queries and, based on the outcome of the queries, define further queries.
Data Mining - Data mining is used to reveal hidden relationships, patterns, and trends in the data warehouse. Data mining is a decision-making technique that is based on a series of analytical techniques taken from the fields of mathematics, statistics, cybernetics, and genetics.

ACID
Atomicity – Is when all the parts of a transaction's execution are either all committed or all rolled back – do it all or not at all
Consistency – Occurs when the database is transformed from one valid state to another valid state. A transaction is allowed only if it follows user-defined integrity constraints.
Isolation – Is the process guaranteeing the results of a transaction are invisible to other transactions until the transaction is complete.
Durability – Ensures the results of a completed transaction are permanent and can survive future system and media failures; that is, once they are done, they cannot be undone.

Software Security
Linus's law: With sufficiently many eyeballs looking at the code, all bugs will become apparent.

Java Security –
Garbage collection – No way to deal with sensitivity of data
Verifier (or Interpreter) – Helps to ensure type safety. It is primarily responsible for memory and bounds checking. Checks each bytecode before loading in JVM for rouge activity.
Class Loader – Loads and unloads classes dynamically from the Java runtime environment. Ensures the external class cannot replace internal classes (class spoofing).
Security Manager – Acts as a security gatekeeper protecting against rogue functionality. Runtime checks on dangerous operations.

Polymorphism – Process objects differently based on the data type
Polyinstantiation - different versions of the same information to exist at different classification levels. Prevents inference attacks.

Common Object Request Broker Architecture (CORBA) - Common Object Request Broker Architecture (CORBA) is a set of standards that address the need for interoperability between hardware and software products. CORBA allows applications to communicate with one another regardless of where they are stored. The ORB is the middleware that establishes a client–server relationship between objects. Using an ORB, a client can transparently locate and activate a method on a server object either on the same machine or across a network. The ORB operates regardless of the processor type or programming language. Not only does the ORB handle all the requests on the system, but it also enforces the system's security policy.

Covert Channel - A covert channel or confinement problem is an information flow issue. It is a communication channel that allows two cooperating processes to transfer information in such a way that it violates the system's security policy.
Types of covert channels: storage and timing
Storage: Sharing of same space by two objects at different security level
Timing: Ability to influence the rate that some other process is able to acquire resources, such as the CPU, memory, or I/O devices.

Memory reuse (Object reuse) - Residual sensitive data on memory location

Malware
Viruses – Replicates itself but needs host to spread. May or may not contain payload.

1. File Infectors – Infects program or object files. Attaches to it. (Jerusalem)
2. Boot sector infectors – Attach or replace boot records.(Brain, stoned or Michelangelo)
3. System Infectors – Attaches to system files or system structure. (Lehigh, MTX, Magistr)
4. Companion virus – Does not physically touch the target file
5. Email Virus – Aware of email system. (Melissa, Loveletter, Hybris, Sircam)
6. Multipartite – Reproduces in more than one way (Nimda, Telefonica, Junkie, One half)
7. Macro Virus – Uses macro programming of app. Infect data files (Concept, CAP, Melissa)
8. Script Virus – Standalone files that can be executed by interpreter.
9. Script host - .vbs as host to script virus.

Worms – Replicates itself but does not require host to attach. (Morris, Loveletter, Nimda, Code red, Lions)
Hoaxes – Warning about new malware that do not exist.
Trojan – Pretends to one thing while performing another unwanted action.
Salami - Stealing in small amounts
Heuristic scanner – Intelligent analysis of unknown code.
Web reputation as protection against Zero day

Software Protection Mechanisms

The **TCB** is the collection of all of the hardware, software, and firmware within a computer system that contains all elements of the system responsible for supporting the security policy and the isolation of objects. When the TCB is enabled, the system is considered to have a trusted path along with a trusted shell. The TCB is responsible for providing the protection mechanisms necessary to ensure that the trusted path cannot be compromised in any way.
The **reference monitor** is considered to be an abstract machine that mediates, or controls, all access that subjects (users) have to objects (data or resources). The security kernel is what actually implements the reference monitor concept.
The **security kernel** is made up of all of the components of the TCB (the software, hardware, and firmware), and it is responsible for implementing and enforcing the reference monitor. A security kernel is responsible for enforcing a security policy.

To be secure, the kernel must meet three basic conditions:
1. Completeness – All accesses to information must go through the kernel
2. Isolation – The kernel itself must be protected from any type of unauthorized access
3. Verifiability – The kernel must be proven to meet design specifications

Protect against buffer overflows - canaries (the use and monitoring of indicator data values at the end of buffer areas)

Process Isolation and Memory Protection
Interrupts and time slicing
Encapsulation of objects
Time multiplexing of shared resources
Naming distinctions
Virtual memory mapping

The memory manager is the function of the operating system that keeps track of how different types of memory are used.
Responsibilities – Relocation, Protection, Sharing, Logical organization, Physical organization
Memory address space protection:

- The first method ensures all system-wide data structures and memory pools used by kernel mode system components can be accessed only while in kernel mode. Thus, user mode requests cannot access these pages.
- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Uses access control lists

TOC/TOU attack - Dependency on the timing of events that takes place in a multitasking operating system. Protection using software locking.
The difference between race conditions and TOC/TOU attacks is subtle but important for the security professional to understand. A race condition implies that two processes will be forced to execute out of sequence, allowing the attacker to control or manipulate the outcome. While a TOC/TOU attack happens as a result of the attackers inserting themselves in between two processes as they are executing, causing a redirection of the second process in some way to control or manipulate the outcome.
TOC/TOU – 2 process, first execute but before second execute use to do something else
Race - 2 process, such way where order can be changed.

Basic Authentication w/ TLS - Simple Base64 encoded password. Must use TLS
Oauth1.0a – Uses cryptographic signature (HMAC-SHA1) – No token passed over wire.
Oauth2 – No Crypto Signature. Communication over TLS.