CISSP Study Guide

CERTIFICATION TRAINING

John Sisler
DATASAGE INC | 321 COMMONS WALK CIR CARY NC 27519

CISSP Study GuideCISSP Study Guide

Contents

Chapter 2 - Cryptography

Cryptography Concepts

Encryption: The process of converting data from plaintext to ciphertext.

Decryption: The process of converting data from ciphertext to plaintext.

Key: A parameter that controls the transformation of plaintext into ciphertext or vice-versa

Synchronous: When encryption or decryption occurs immediately.

Asynchronous: When encryption or decryption requests are processed from a queue.

Symmetric: When a single private key both encrypts and decrypts the data.

Symmetrical: same key for encrypting and decrypting.

Asymmetrical: When a key pair (one private and one public) performs encrypting and decrypting.

Digital Signature: Provides sender authentication and message integrity. The message acts as an input to a hash function, and the sender's private key encrypts the hash value. A hash computation on the received message determines the validity of the message.

Hash: A one-way function that reduces a message to a hash value. A comparison of the sender's hash value to the receiver's hash value determines message integrity.

Digital Certificate: An electronic document that identifies the certificate holder.

Plaintext: A message in its original format.

Ciphertext: An altered form of a message that is unreadable without knowing the key and the encryption system used; also, referred to as a cryptogram

Cryptosystem: The components that make encryption possible, including the algorithm, key, and key management functions.

Cryptanalysis: The science of decrypting ciphertext without prior knowledge of the key or cryptosystem used.

Key Clustering: This occurs when different encryption keys generate the same plaintext message.

Keyspace: All the possible key values when using a particular algorithm or security measure.

Collision: An event that occurs when a hash function produces the same hash value on different messages.

Algorithm: A mathematical function that encrypts and decryypts data; also referred to as a cipher.

Cryptology: The science that studies encrypted communication and data.

Encoding: synonym of Encrypting

Decoding: synonym of Decrypting

Transposition: The process of shuffling or reordering the plaintext to hide the original message; also, referred to as permutation.

Substitution: The process of exchanging 1 byte in a message for another.

Confusion: The process of changing a key value during each round of encryption. Confusion is often carried out by substitution.

Diffusion: The process of changing the location of the plaintext within the ciphertext. Diffusion often uses transposition.

Avalanche effect: The condition in which any change in the key or plaintext, no matter how minor, will significantly change the ciphertext

Work factor: The amount of time and resources that would be needed to break the encryption.

One-way function: A mathematical function that can be more easily performed in one direction than in the other.

Trapdoor: A secret mechanism that allows the implementation of the reverse function in a one-way function.

Cryptographic Life Cycle:

1. Implementation
2. Maintenance
3. Retirement or Replacement

XOR: In cryptography, the simple XOR cipher is a type of additive cipher, an encryption algorithm that operates per the principles:

$$A \oplus 0 = A,$$

$$A \oplus A = 0,$$

$$(A \oplus B) \oplus C = A \oplus (B \oplus C),$$

$$(B \oplus A) \oplus A = B \oplus 0 = B,$$

where $\oplus$ denotes the exclusive disjunction (XOR) operation. This operation is sometimes called modulus 2 addition (or subtraction, which is identical). With this logic, a string of text can be encrypted by applying the bitwise XOR operator to every character using a given key. To decrypt the output, merely reapplying the XOR function with the key will remove the cipher.

Cryptography History

Earliest forms were some sort of substitution cipher, where each character in the alphabet was replaced with another.

Mono-Alphabetic: A substitution cipher using one alphabet

Polyalphabetic: A substitution cipher using many alphabets

Scytale Cipher: The Spartans created this cipher, which used a sheet of papyrus wrapped around a wooden rod. The encrypted message had to be wrapped around a rod of the correct size to be deciphered.

Caesar's Cipher: A mono-alphabetic cipher that shifts the letters of the alphabet in three places. It is easily reverse engineered, thus led to the development of the polyalphabetic ciphers.

Vingenere Cipher: One of the first polyalphabetic ciphers. It uses 27 shift alphabets with letters being shifted up one place. This shifting is referred to as a Vingenere table. To encrypt a message, you must know the security key. The security key is then used with the plaintext message to determine the ciphertext.

Kerchoff's Principle: the key is secret and the algorithm is known.

- System must be practically, if not mathematically, indecipherable.
- It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
- Key must be communicable and retained without the help of written notes, and changeable or modifiable at the will of the correspondents.
- Must be applicable to telegraphic correspondence.
- Must be portable, and its usage and function must not require the concourse of several people.
- System needs to be easy to use, requiring neither mental strain or the knowledge of a long series of rules to observe.

Enigma: Encryption machines used during WWII that consisted of rotors and a plug board.

- To encrypt the operator would configure the initial settings
- Then the operator would type each letter of the plaintext message into the machine one at a time, resulting in the generation of a different letter
- After recording the ciphertext letter, the operator would advance the rotors to a new setting and enter another
- With each letter entered, the operator had to change the machine setting
- The key was the initial machine setting and the series of increments used to advance the rotor, both of which had to be known by the receiver to properly convert the ciphertext intro plaintext.

Lucifer: Lucifer by IBM developed complex mathematical equations there were later used by the U.S. National Security Agency in the development of the U.S. Data Encryption Standard (DES), which is still used today in some forms.

- Used a Feistel cipher, an iterated block cipher that encrypts plaintext by breaking the block into two halves.
- Then a round of transformation is applied to one of the halves using a subkey
- Output is XORed with the other block half
- Finally, the two halves are swapped to complete the round.

Cryptosystem Features

- Consists of software, protocols, algorithms, and keys
- Strength comes from the algorithm and the length and secrecy of the key.
- Provides authentication, confidentiality, integrity, authorization, and nonrepudiation.
- Does not directly endure data availability
- Provides authentication by determining the sender's identity and validity using digital signatures.
- Provides confidentiality through encryption
- Provides integrity with hash functions, which do not prevent data alteration but provide a means to determine it has occurred.

- Provides authorization by providing a key to a valid user that will allow the user to access a resource.
- Nonrepudiation prevents the sender from denying that s/he sent the message; provided by public key cryptography and digital signatures.

Encryption Systems

Running Key Cipher: Uses a physical component, usually a book, to provide the polyalphabetic characters; also, referred to as key ciphers.

- Indicator Block: identifies the location in the book the originator started
- Parties must agree upon which book to use and where the indicator block will be included in the cipher message

Concealment Cipher: Plaintext is interspersed somewhere within other written material

- Parties must agree on the key value, which defines which letters are part of the actual message; belongs to the stenography realm.

Substitution Ciphers: Uses a key to substitute characters or character blocks with different characters or character blocks.

Caesar's and Vingenere's Ciphers are two of the earliest forms of substitution ciphers.

Modulo 26 substitution cipher uses letters of the alphabet numbered in order starting at 0

- The sender takes the original message and determines the number of each letter in the original message
- Then the letter value for the keys are added to the original letter values
- The value result is then converted back to text.

Transposition Ciphers: Scrambles the letters of the original message in a different order. The key determines the positions to which the letters are moved.

Symmetric Algorithms: These use a private or secret key that must remain secret between the two parties. Each pair requires a separate private key.

- To calculate the number of keys needed, you would *U(U-1)/2* where U us the number of users.
- The key must remain secure
- Communicating the secret key requires an out-of-band method (physical contact, courier, etc.)
- Session key encrypts messages between two users during one communication session.
- Synonyms: single-key, secret-key, private-key, or shared key cryptography
- Provide confidentiality but not authentication or nonrepudiation
- Include DES, AES, IDEA, Skipjack, Blowfish, Twofish, RC4/5/6, and CAST

Stream Based Symmetric Algorithms: Perform encryption on a bit-by-bit basis and use keystream generators that create a but stream that is XORed with the plaintext bits; example RC4. The result of the XOR operation is the ciphertext

Advantages of stream based ciphers are:

- Have lower error propagation because encryption occurs on each bit
- Popular in hardware implementations
- Use the same key for encryption and decryption
- Cheaper to implement than block ciphers
- Employ only confusion.

Block Symmetric Algorithms: These perform encryption by breaking the message into fixed-length units; examples are IDEA, Blowfish and, RC5/6.

- Easier to implement than stream-based
- Less susceptible to security issues
- Popular in software implementations
- Employ both confusion and diffusion
- Modes include: ECB, CBC, CFB, and CTR
- Initialization Vectors (Ivs) are used by the modes to ensure that patterns are not produced during encryption by using random values with the algorithms.

Asymmetric Algorithms: Use both a public and private key.

- The public key is known to all parties and the private key is only known by its owner
- One key encrypts the message, and the other decrypts the message
- Deriving the private key from the public key is virtually impossible even though the keys are mathematically related.
- Provides confidentiality, integrity, authentication, and nonrepudiation.
- For confidentiality, the message should be encrypted with the receiver's public key; this is known as secure message format.
- For authentication, a message should be encrypted with the sender's private key; known as open message format.
- Includes Diffie-Hellman, RSA, El Gamal, ECC, Knapsack, DSA, and Zero Knowledge Proof.

Hybrid Ciphers: Use both types of algorithms to provide confidentiality, authentication, and nonrepudiation.

Hybrid Cipher Process

1. Symmetric algorithm provides the keys used for encryption
2. Symmetric keys are then passed to the asymmetric algorithm, which encrypts the symmetric keys and distributes them
3. Message is then encrypted with the symmetric key
4. Message and the key are sent to the receiver
5. Receiver decrypts the symmetric key and uses it to decrypt the message

Best use for hybrid encryption is when parties do not have a shared secret key and large quantities of sensitive data must be transmitted.

Substitution Ciphers

Substitution Cipher: These use a key to substitute characters or character blocks with different character or character blocks

One-Time-Pad: most secure because the key value is added to the value of the letters, using a key the same length as the plaintext message; then the following conditions must be met:

- Must be used only one time
- Must be as long as (or longer) than the message
- Must consist of random values
- Must be securely distributed
- Must be protected at its source and destination

Steganography: This is when a message is hidden inside another object, such as a picture or a document. Steganography methods include Concealment Ciphers and Digital Watermarking to deter unauthorized use.

Symmetric Algorithms

Digital Encryption Standard (DES): This is a Symmetric system created by the NSA based on the 128-bit Lucifer algorithm by IBM

DES

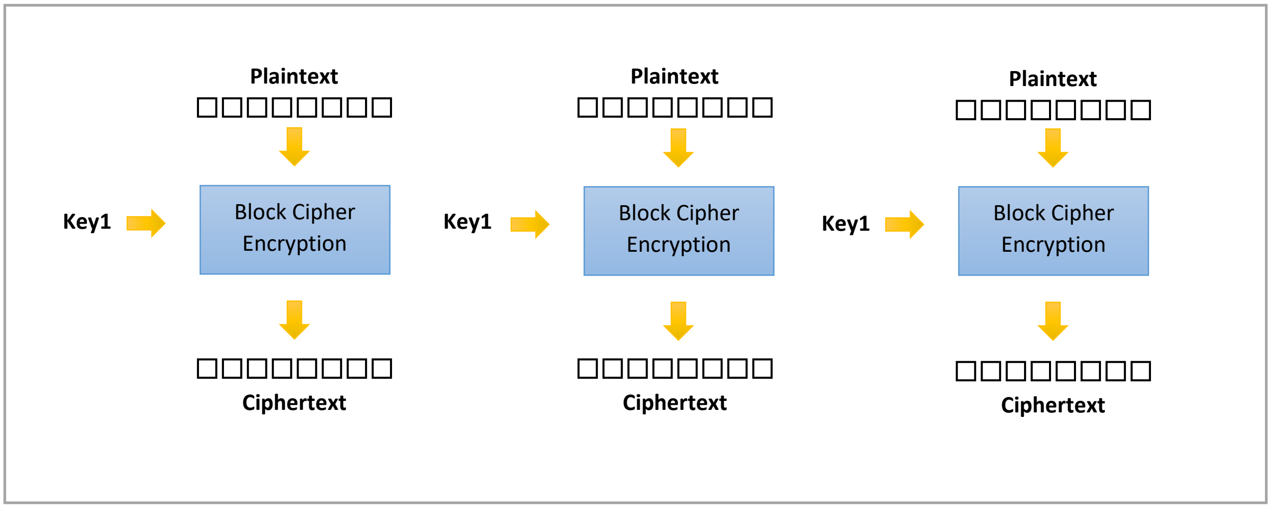
1. Uses a 64-bit key, 8 bits of which are used for parity, yielding an effective key length of 56 bits
2. Divides the messages into 64-bit blocks
3. 16 rounds of transposition and substitution are performed on each block, resulting in a 64-bit block of ciphertext
4. Replaced by 3DES and AES
5. DES-X is a variant of DES that uses multiple 64-bit keys in addition to the 56-bit DES key

6. Double-DES, using 112-bit keys, is obsolete after an attack reduced its security to match DES

5 Modes of DES

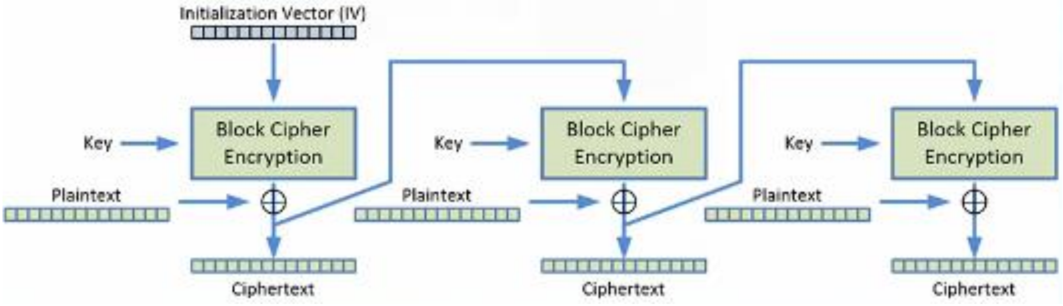
Mode 1 Electronic Code Book (ECB)

- 64-bit blocks of data are processed by the algorithm using the key
- The ciphertext produced can be padded to ensure the result is a 64-bit block
- Encryption errors only affect individual blocks
- ECB is run in parallel so it is fast
- Not good for large messages since the same key is reused a pattern may emerge
- Smaller messages lengths like databases can use this method



Mode 2: Cipher Block Chaining (CBC)

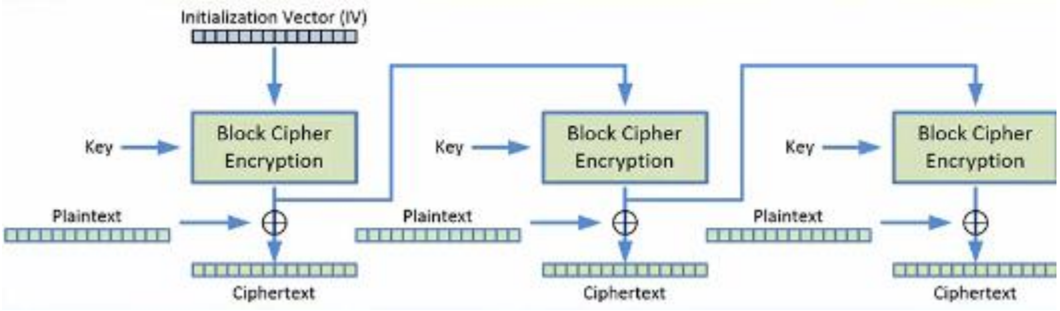
- Works with 8-bit (or smaller) blocks and uses a combination of stream ciphering and block ciphering
- Ciphertext block must be the same size as the plaintext block
- Encryption errors will affect any future block encryption
- Should not be used to encrypt video or voice signals
- This problem led to the need for DES OFB mode



Mode:3 (CFB) – replay?

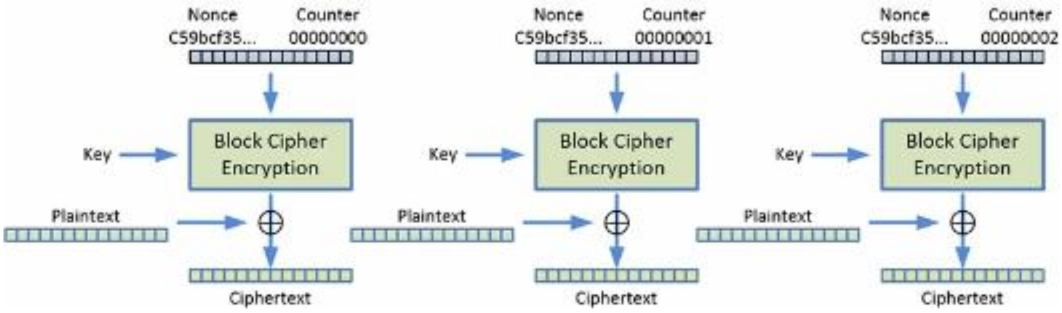
Mode 4: Output Feedback (OFB)

- Works with 8-bit (or smaller) blocks and uses a combination of stream ciphering and block ciphering, using the previous keystream with the key to create a new keystream.
- Size of the keystream value must be the same size as the plaintext block
- Less susceptible to the error type that CFB has



Mode 5: Counter Mode (CTR)

- Like OFB mode, but uses an incrementing IV counter to endure that each block is encrypted with a unique keystream
- Ciphertext is not chaining into the encryption process
- Performance is much better than the other modes



Triple DES (3DES)

A version of DES that increases security by using three 56-bit keys.   to 3 times slower than DES but replaced it temporarily.

Four modes are:

1. 3DES-EEE3: Each block of data is encrypted 3 times, each with a different key
2. 3DES-EDE3: Each block of data is encrypted with the key 1, decrypted with key 2, then encrypted with key 3
3. 3DES-EEE2: Each block of data is encrypted with the key 1, encrypted with key 2, then encrypted again with key 1
4. 3DES-EDE2: Each block of data is encrypted with the key 1, decrypted with key 2, then encrypted again with key 1

Advanced Encryption Standard (AES)

This the DES replacement that uses the Rijndael algorithm and supports 3 bit key sizes. It is currently the required algorithm for sensitive but unclassified U.S. government data.

1. 128-bit key with 128 block size that undergoes 10 transformation rounds
2. 192-bit key with 192 block size that undergoes 12 transformation rounds
3. 256-bit key with 256 block size that undergoes 14 transformation rounds

International Data Encryption Algorithm (IDEA)

- Block cipher uses 64-bit blocks
- Each block is divided into 16 smaller blocks
- Uses a 128-bit key and performs 8 rounds of transformation on each of the 16 blocks
- Faster encrypting and harder to break than DES, but not as popular as DES or AES because it was patented until 2012
- Used in PGP

Skipjack

- Block-cipher, symmetric algorithm developed by the NSA
- Uses an 80-bit key that encrypts 64-bit blocks
- Made for Clipper Chip but since algorithm is classified and NSA had backdoor nobody wanted it.

Blowfish

- Block-cipher that uses 64-bit data blocks using anywhere from 32-bit to 448-bit encryption keys
- Performs 16 rounds of transformation
- Developed to replace DES and is one of the few algorithms not patented

Twofish

- Version of Blowfish that uses a 128-bit data blocks using 128, 192, and 256-bit keys
- Uses 16 rounds of transformation
- Not patented

RC4 or ARC4

- One of the most popular stream ciphers
- Used in SSL and WEP
- Uses a variable key size of 40 to 2048 bits and up to 256 rounds of transformation

RC5

Block cipher that support keys up to 2048 bits and up to 255 rounds of transformation

- Supported block sizes are 32, 64, or 128 bits

- Industry often uses RC5 = w/r/b
  - W is the block size
  - R is the number of rounds, and
  - B is the number of 8-bit bytes in the key

RC6

Block cipher based on RC5 and uses the same key size, rounds, and block size.

- Originally developed as an AES solution but lost the contest to Rijndael
- Faster than RC5

CAST

Block cipher wit 2 versions:

1. CAST-128: 40 to 128-bit key, 12 or 16 rounds of transformation on 64-bit blocks
2. CAST-256: 128 to 256-bit key, 48 rounds of transformation on 128-bit blocks

Asymmetric Algorithms

Diffie-Hellman

An asymmetric key arrangement algorithm that is responsible for the key agreement process

- Provides secure key distribution, but not confidentiality, authentication, or nonrepudiation
- Susceptible to man-in-the-middle attacks unless an organization implements digital signatures or digital certificates for authentication at the beginning of the Diffie-Hellman process

Key Agreement Process

1. Jim generates a private and public key, and Sue generates a private and public key
2. Jim and Sue share their keys with each other
3. Diffie-Hellman is applied to John's private key and Sally's public key on Sue's machine
4. Thus, the same shared value is created for John and Sally, which in turn creates the same symmetric key on each system using the asymmetric key agreement algorithm

RSA

Most popular asymmetric algorithm and can provide key exchange, encryption, and digital signatures

1. Uses 1024 = 4096-bit key and performs one round of transformation
2. If factorization of prime numbers is used the implementation is considered breakable
3. Uses a one-way function to provide en/decryption and digital signature generation/verification
   1. The public key works with the one-way function to perform encryption and digital signature verification
   2. The private key works with the one-way function to perform decryption and signature generation
4. Attackers can use a Number Field Sieve (NFS) factoring algorithm to attach RSA

El Gamal

this is based on the Diffie-Hellman algorithm

- Deals with discrete logarithms and can provide key exchange, encryption, and digital signatures
- Any key size can be used but it is the slowest algorithm so smaller than 1024 is wise

Elliptic Curve Cryptosystem (ECC)

this provides secure key distribution, encryption, and digital signatures

- Any key size can be used, and can use a key much smaller than RSA, or other asymmetric algorithm, while providing comparable security
- Benefits are speed and efficiency and even better security that RSA when using comparable key sizes

Knapsack

A series of asymmetric algorithms that provide encryption and digital signatures, but is obsolete.

Zero Knowledge Proof

Technique used to ensure that only the minimum needed information is disclosed

> If the sender encrypts data with their private key and the receiver decrypts with the originator's public key, then the originator proves that they have the private key simply because they can read the message.

Message Integrity

Message Integrity: This ensures that a message has not been altered by using:

1. Parity bits: This adds an extra bit to the data indicating if the number of bits is odd or even and is confirmed on arrival
2. Cyclic Redundancy Checks (CRC): This uses polynomial division to determine the CRC value, which is usually 16 or 32-bits long. CRC will not match if even one bit is incorrect
3. Checksum: This adds up the bytes of data being sent and then compares the source and receiving checksum values.

Hash Functions

- One-Way Hash: for this to be effective, creating two different messages with the same hash value must be mathematically impossible to prevent collisions
- Hashing algorithm is publicly known
- Function is always performed in one direction; using it in reverse in unnecessary
- A weakness is an attacker could capture and alter the original message to create a second invalid message with a new hash value. The invalid message will look valid because the invalid message was appended with the attacker's new hash value, not the original hash value
- Message Authentication Code (MAC): encrypts the has function with a symmetric key algorithm creating a Keyed MAC
    - The symmetric key does not encrypt the original message; it only protects the hash value

Message Digest Algorithms

- MD2: 128-bit hash using 18 rounds of computations
- MD4: 128-bit hash using 3 rounds of computations - compromised
- MD5: 128-bit hash using 4 rounds of computations
    - Not collision free so it is not good for SSL or digital signatures
    - U.S. government requires usage of SHA-2 instead of MD5
    - Used commonly by software vendors when releasing patches so customers can verify integrity

- MD6: variable has value and variable computations
  - Introduced as a candidate for SHA-3 but withdrawn; algorithm susceptible to differential attacks
  - This has been re-released with a patch but was too late to be accepted as the NIST SHA-3 standard
- SHA: This is a family of 4 algorithms published by the U.S. NIST
  - SHA-0: 160-bit hash value with 80 rounds of computation on 512-bit blocks
  - SHA-1: update to SHA-0 that addresses compromises
  - SHA-2: has its own family of functions including
    - SHA-224: 224-bit hash, 64 rounds of computations on 512-bit blocks
    - SHA-256: 256-bit hash, 64 rounds of computations on 512-bit blocks
    - SHA-384: 384-bit hash, 80 rounds of computations on 1024-bit blocks
    - SHA-512: 512-bit hash, 80 rounds of computations on 1024-bit blocks
    - SHA-512/224: 224-bit hash, 80 rounds of computations on 1024-bit blocks
    - SHA-512/256: 256-bit hash, 80 rounds of computations on 1024-bit blocks
  - SHA-3: Family of hash functions proactively drafted by NIST in 2014.
    - Hash value sizes range from224 to 512-bits and defaults to 120 rounds of computations
  - HAVAL: customized combinations include:
    - 128, 160, 192, 224, and 256 bit hashes
    - Computation rounds can be 3, 4, or 5
    - Collision issues have been discovered
  - RIPEMD-160: 160-bit hash after performing 160 rounds of computations on 512-bit blocks
  - Tiger: 128, 160, or 192-bit hash after 24 rounds on 512-bit blocks
    - 192 is popular
    - Unlike MD5, RIPEMD, SHA-0, and SHA-1, Tiger id not built on the MD4 architecture

  - Message Authentication Code (MAC)

    - Hash MAC (HMAC): this is a keyed-hash MAC that involves a hash function with a symmetric key
    - Any hash function can be used (i.e. HMAC SHA-1)
    - Strength depends on the hash function, including the hash value size and the key size
  - Cipher Block Chaining: MAC (CBC-MAC) is a block cipher operating in CBC mode providing integrity and authentication
  - Cipher-Based MAC (CMAC): operates like CBC-MAC with better mathematical functions
    - Superior math addresses security issues
    - CMAC is approved to work with AES and 3 DES

Digital Signatures

Digital Signatures are:

- A hash value encrypted with the sender's private key
- Provides authentication, nonrepudiation, and integrity
- Public key cryptography used to create digital signatures
- Users register their public keys with a certification authority (CA), which distributes a certificate containing the user's public key and the CA digital signature
- Digital signature is computed by the user's public key and validity period being combined with the certificate issuer and digital signature algorithm identifier

Blind Signature: A form of digital signature where the contents of the message are masked before it is signed

Digital Signature Standard (DSS): this is a federal digital security standard that governs the Digital Security Algorithm (DSA), which generates a message digest of 160 bits

- U.S. Federal government requires the use of DSA, RSA, or Elliptic Curve DSA (ECDSA) and SHA for digital signatures
- RSA provides digital signatures, encryption, and secure symmetric key distribution

Public Key Infrastructure (PKI)

Public Key Infrastructure includes systems, software, and communication protocols that distribute, manage, and control public key cryptography

- Can certify that a public key is tied to an entity and verify that a public key is valid
- X.509: This framework enables authentication between networks and over the internet
- Includes timestamping and certificate revocation to endure that the certificates are managed properly
- Provides confidentiality, message integrity, authentication, and nonrepudiation
- Structure include:
    - Certificate Authorities (CA's): Creates/signs digital certificates then maintains and revokes the certificates
    - Certificates: Binds the party to the public key
    - Public CA: Provide PKI as a payable service to companies who need them
    - Private CA: Operated by the enterprise so that the organization can control all aspects of the PKI process
    - Registration Authorities: Verifies the requestor's identity and registers the requestor passing the request to the CA
    - Certificate Revocation Lists (CRL): maintained lists of revoked keys; browser checked and pushed from clients
    - Cross-Certification: Establishes a trust relationship between two CA's
    - Certification Path Validation: Checking the legitimacy of all signatures on the certificates in the certification path
    - Online Certificate Status Protocol (OCSP): This protocol obtains the revocation status of an X.509 cert.
        - This is an alternative to the CRL used by many PKI's
        - Automatically validates and reported back the status by accessing the CRL
    - Certificate provides entity with the credentials to prove its identity and associates that identity with a public key by providing:
        - Serial number,
        - Issuer,
        - Subject (owner), and
        - Public Key
    - Verisign first introduced the following digital certificate classes:
        - Class 1: For individuals and intended for email and can be saved by web browsers
        - Class 2: For organizations that must provide proof of identity
        - Class 3: For servers and software signing in which independent verification and identity/authority checking is done by the issuing CA

- Revocation Request Grace Period: Maximum amount of time between a revocation request and the revocation
    - Shorter time has more security but a more expensive implementation costs

Process to Request a Certificate

1. User requests a digital certificate, and the RA receives the request
2. RA requests identifying information from the requestor
3. RA forwards the certificate request to the CA
4. CA creates a digital certificate for the requestor, including the public key and identity information
5. User receives the certificate

Process for communicating between entities

1. User 1 requests User 2's public key from the certificate repository
2. Repository sends User 2's digital certificate to User 1
3. User 1 verifies the certificate and extracts User 2's public key
4. User 1 encrypts the session key with User 2's public key and sends the encrypted session key and User 1's certificate to User 2
5. User 2 receives User 1's certificate and verifies the certificate with a trusted CA

Now the two entities can communicate using encryption

Key Management

Key Management is essential to ensure that the cryptography provides:

- Confidentiality
- Integrity
- Authentication

Involves ensuring that the keys are protected during:

- Creation
- Distribution
- Transmission

- Storage

Keys should always be stored in ciphertext when stored on a non-cryptographic device

Key distribution, storage, and maintenance should be automatic by integrating the process into the application

Backup keys should be made stored in a secure location

Designated individual should have control of the backup copies with other individuals designated as emergency backups

Key Recovery Process

Key Recovery Process should require more than on operator to ensure that only valid key recovery requests are completed or keys should be broken into parts and deposited with trusted agents, who provide their part of the key to a central key authority when authorized to do so.

Key recovery personal should span across the entire organization and not just be members of the IT department

Limit the number of keys that are used and therefore must be protected

When designing the key management process:

1. Securely store and transmit the keys
2. Use random keys
3. Issue keys of sufficient length to ensure protection
4. Properly destroy keys when no longer needed
5. Backup the keys to ensure that they can be recovered

Trusted Platform Module

Trusted Platform Module (TPM): A security chip installed on a computer motherboard that is responsible for managing symmetric and asymmetric keys, hashes, and digital certificates

- It helps protect passwords, encrypt drives, and manage digital rights, making it much harder for attackers to gain access to the computers that have an enabled TPM-chip

- Uses include:
    - Binding: this step binds the hard drive to a computer using encryption
    - Sealing: this step seals the system state to its unique hardware and software configuration
- The system can boot only after the TPM verifies integrity of the boot computed hash value to the original hash value
- Uses both static memory and dynamic memory to retain important information when the computer is turned off
- The memory used in a TPM chip is:
    - Endorsement Key (EK): Persistent memory installed by the manufacturer containing a public/private key pair
    - Storage Root Key (SRK): Persistent memory that secures keys stored in the TPM
    - Attestation Identity Key (AIK): Dynamic memory that ensures the integrity of the EK
    - Platform Configuration Register (PCR) Hashes: Dynamic memory that stores data hashes for sealing
    - Storage keys: Dynamic memory that contains the keys used to encrypt storage (i.e. HDD, Flash, etc.)

Encryption Communication Levels

Link Encryption

Encrypts all the data transmitted over a link

- Data Link Control information, which is needed to transmit the data properly is the only part not encrypted
- Header information is decrypted so that routing can occur and then re-encrypts before sending the information to the next device
- Used to ensure data security and privacy over a public communication link
- Protects against packet sniffers and other eavesdropping
- All the data is encrypted, and no user interaction is needed for it to be used
- Each device that the data must be transmitted through must:
    - Receive the key
    - Key changes must be transmitted to each device on the route
    - Packets are decrypted at each device

End-to-End Encryption

This encrypts less of the packet information

- Packet routing information, headers, and addresses are not encrypted
- Advantages are flexibility to select exactly what gets encrypted and how
- Every device does not have to perform en-decryption to determine how to route the packet

Email Security

Pretty Good Privacy (PGP): Provides email encryption using different technologies based on organizational needs

- Can provide confidentiality, integrity, and authenticity depending on which methods are used
- Provides key management using RSA and a web of trust
- Public keys of all the users are stored on each user's computer in a keyring file
- Each keyring file has the user's assigned level of trust
- The users within the web of trust vouch for each other

- User can choose the initial trust level and can change that level later if circumstances warrant so
- Compromise of a user's public key requires the key is removed from the ring of all users
- Provides data encryption for confidentiality using IDEA
- When used with MD5 it provides data integrity
- When used with public certificate it provides authentication

Secure MIME (S/MIME): This allows MIME to encrypt and digitally sign email messages and encrypt attachments

- Adheres to the Public Key Cryptography Standards (PKCS), which is a set of public-key cryptography standards designed by the owners of the RSA algorithm
- Uses:
  - Encryption for confidentiality,
  - Hashing for integrity,
  - Public key certificates for authentication, and
  - Message Digests to provide nonrepudiation
- Quantum Cryptography: This method combines quantum physics and cryptography offering the ability to factor large prime numbers
  - Provides strong encryption and eavesdropping detection
  - Excellent choice for organizations that transmit Top Secret data, including the U.S. government

Internet Security

Remote Access: This allows a user to access resources from a remote location

- Organizations ensure that the data is protected
- Remote Access Servers can require encrypted connections with remote access clients

Secure Socket Layer (SSL): This protocol provides encryption, server/client authentication, and message integrity

- 40-bit (SSL 2.0) or 128-bit (SSL 3.0); 40-bit is susceptible to attacks
- Allows applications to have encrypted and authenticated communication across a network

Transport Layer Security (TSL): This is an open community standard that provides many SSL services

- Based on SSL 3.0 but more extensible
- Designed for privacy and data integrity between two communicating applications

HTTPS: HTTP running over an SSL or TSL protocol

Secure HTTP (S-HTTP): Encrypts a single communication message, not an entire session or conversation, but us uncommon

Secure Electronic Transaction (SET): This secures credit card transactions based on X.509 certificates and asymmetric keys

- Never fully adopted; required full cooperation of banks, cc users, wholesalers/retailers and payment gateways

Cookies: These are text files stored on a user's HDD or in memory and contain information about the user's Internet habits.

- Malicious sites can use cookies to discover information about a user.

Secure Shell (SSH): This is an application/protocol that is used to remotely log in to another computer over a secure tunnel

Internet Protocol Security (IPsec): Suite of protocols that establishes a secure channel between two devices:

- AH: provides authentication and integrity
- ESP: provides authentication, integrity, and encryption (confidentiality)
- Security Association (SA): records a device's configuration that needs to participate in IPsec communication
- Security Parameter Index (SPI): table that tracks the different SA's used and ensures that a device uses the appropriate SA to communicate with another device

IPsec has two modes:

1. Transport Mode: protects only the message payload
2. Tunnel Mode: protects the payload, routing and header information

Both modes can be used for gateway-to-gateway IPsec communication

Internet Key Exchange (IKE): Key exchange method most commonly used by IPsec which is a combination of OAKLEY and Internet Security Association and Key Management Protocol (ISAKMP)

Authentication methods used by IKE include:

- Pre-Shared keys, certificates, and public key authentication
- Most secure implementation of pre-shared keys require a PKI, but simple passwords can be used

Cryptography Attacks

Passive Attacks: implemented to discover information and is much harder to detect because it is usually carried out by eavesdropping or packet sniffing

Active Attacks: involve an attacker carrying out steps, like message alteration or file modification

Cryptography is usually attacked via the key, algorithm, execution data, or people, with most attempts attacking keys.

Ciphertext-Only Attack: An attacker uses several encrypted messaged to figure out the key used in the encryption process

Known Plaintext Attack: An attacker uses the plaintext and ciphertext versions of a message to discover the key using reverse engineering, frequency analysis, or brute force to determine the kay so that all messages can be deciphered

Chosen Plaintext Attack: An attacker sends a message hoping that the user will forward that message as ciphertext to another user. The attacker captures the ciphertext version of the message to compare

Chosen Ciphertext Attack: An attacker chooses the ciphertext to be decrypted to obtain the plaintext. This attack is more difficult because control of the system that implements the algorithm is needed.

Social Engineering Attack: An attacker attempts to trick users into giving their attacker the cryptographic key used

Brute Force: Uses all possible keys until a key is discovered

Differential Cryptanalysis: a.k.a. Side-Channel attacks measure the execution times and power required by the cryptographic device to help determine the key and algorithm used

Linear Cryptanalysis: A known plaintext attack that uses linear approximation, which describes the block cipher behavior

Algebraic Attack: Exploits known vulnerabilities of the algebra used, looking for those vulnerabilities can help the attacker determine the key and algorithm used

Frequency Analysis: Relies on the fact that substitution and transposition ciphers will result in repeated patterns in ciphertext. Today's algorithms are considered too complex to be susceptible to this form of attack but, as technologies advance, this could change.

Birthday Attack: Assumes that finding two messages with the same hash value is easier than matching a message with its hash value; most hash algorithms resist birthday attacks.

Dictionary Attacks: Uses all the words in the dictionary until a key is discovered that decrypts the ciphertext correctly.

Replay Attacks: Attacker sends the same data in an attempt to trick the reciving device, most commonly authentication information; countermeasures for this are timstamps and sequence numbers

Analytic Attack: An attacker uses known structural weaknesses or flaws to determine the algorithm used

Statistical Attack: An attacker uses known statistical weaknesses of an algorithm to aid in the attack

Factoring Attack: This is carried out against the RSA algorithm by using the solutions of factoring large numbers

Reverse Engineering: attacker purchases a particular cryptographic product to attempt to discover the algorithm used

Meet-in-the-Middle Attack: An attacker tries to break the algorithm by encrypting from one wnd tna decrypting from the other to determine the mathematical problem used.

Chapter 3 – Physical Security

Threat Mitigation Techniques

Internal: Address threats from those who might have access to the room or building

- E.g. A server room door's card swipe lock protects the room from people already in the building

External: Address maintain perimeter security or building access from outsiders

- E.g. An electric fence surrounding the facility

Geographical Man Made and Political Threats

Natural Threats and Mitigation

- Hurricanes: Location, rate of occurrence, and severity should dictate investment
- Tornadoes: Location, rate of occurrence, and severity should dictate investment
- Earthquakes: Location, rate of occurrence, and severity should dictate investment
- Floods: Keep computing equipment off the ground floor and build raised flooring
- Electrical
    - Mission Critical systems should have UPS
    - Onsite generators for long term power
    - Relative humidity range 40% - 60%
    - Line conditioners

Communications

- Fault tolerant Internet connections
- Home and Mobile employee numbers
- Establish radio communication for campus with repeater antennas for emergencies

Man-Made Threats

Explosions: Prevent access to areas where explosions can do significant damage

Fire

- All walls should have a 2-hour minimum fire rating
- Deploy auxiliary alarms
- Use proper extinguisher or suppression system

Vandalism: Endure critical components are inaccessible

Fraud: Prevent physical access to critical systems

Theft: Prevent physical access to the facility

Collusion: Collaboration to negotiate an otherwise separation of duties

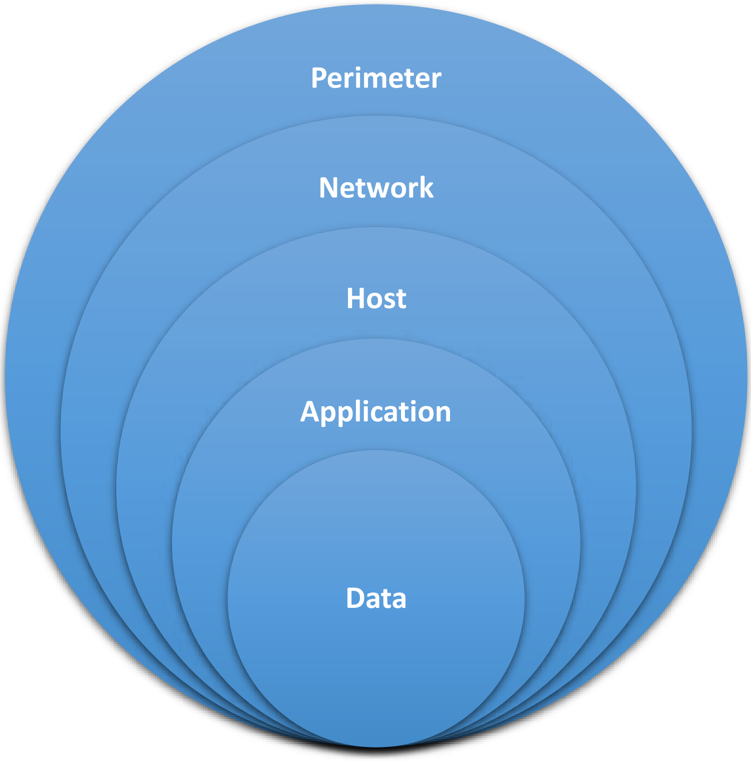
Politically Motivated Threats

- Strikes: Can cost productivity and can hurt the image of the company
- Riots: The enterprise is seen as a willing participant in some perceived slight
- Civil Disobedience: Physical security of the facility becomes important to prevent harm to the facility
- Terrorists Acts: Emergency planning and rehearsals
- Bombing: Evacuation plans

Site and Facility Design

Layered Defense Model

In such a model, reliance should not be based on any single physical security concept but on the use of multiple approaches that support one another.



Crime Prevention Through Environmental Design (CPTED)

CPTED refers to designing the facility from the ground up to support security

1. Natural Access Control: This encompasses placement of the doors, lights, fences, and landscaping to satisfy security goals in the least obtrusive and aesthetically appealing manner

2. Natural Surveillance: This promotes visibility of all areas to discourage crime
3. Natural Territorial Reinforcement: This promotes feeling of community in the area and attempts to extend the sense of ownership to the employees

Physical Security Plan Goals

- Deter Criminal Activity: Layout and supporting policies should deter crime.
- Delay Intruders: Add impediments to entry and implement procedures to slow and monitor people
- Detect Intruders: Systems and procedures should be in place that allow for criminal activity to be detected
- Assess Situation: Identify specific personnel to alert and actions to be taken during an event
- Respond to Intrusion: Anticipate and develop appropriate responses to intruders and to common disruptions

Facility Selection Issues

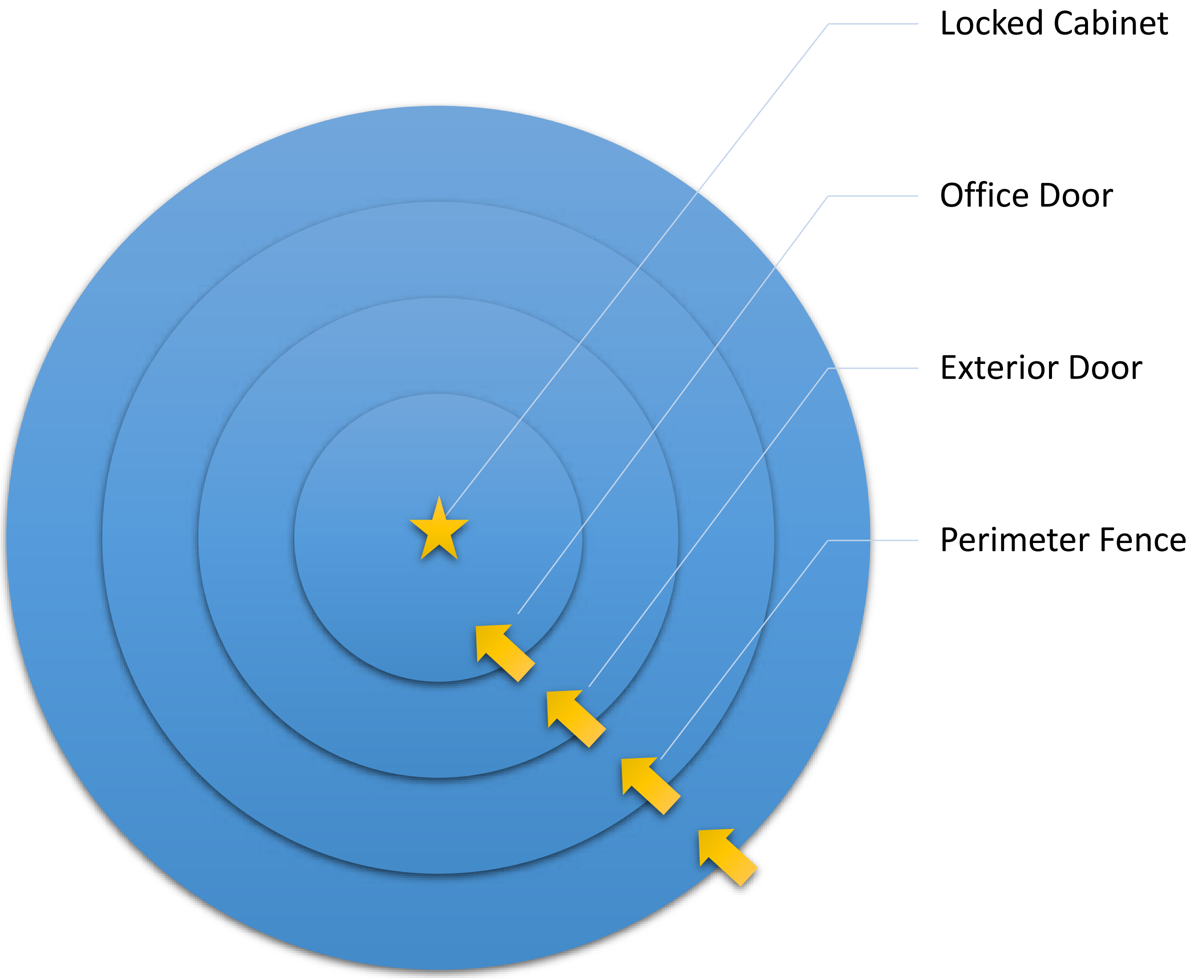
- Visibility: Amount of visibility desired depends on the organization and the facility processes
- Surrounding Area and External Entities: Consider the nature of the operations of surrounding businesses
- Accessibility: Ease with which employees and officers can access the facility is a consideration
- Construction: Consideration of the support system built into the building
- Internal Compartments: All rooms that need to be secured should not have drop ceilings

Computer and Equipment Rooms

Should be locked at all times and secured with the following safeguards:

- Should be in the center of the building, when possible
- Should have a single access door or entry point
- Avoid the top floor of buildings
- Install and frequently test fire detection and suppression systems
- Install raised flooring
- Install separate power supplies
- Use only solid doors

Perimeter Security



Barriers or Bollards

Protection from Vehicles

Fences and Gates

3-4 feet tall only deter casual intruders

6-7 feet tall are too tall to climb easily

8 feet and taller deter more determined intruders, particularly when augmented by razor wire

Gates:

- Class 1: Residential
- Class 2: Commercial
- Class 3: Industrial
- Class 4: Restricted Areas

Perimeter Intrusion Detection Systems

Infrared Sensors: Identify changes in heat waves

Electromechanical Systems: Operate by detecting a break in an electrical circuit

Photometric or Photoelectric Systems: Operate by detecting changes in the light so are used in windowless areas

Acoustical Systems: Use strategically places microphones to detect and sound made during a forced entry

Wave Motion: Generates a wave patter in the area to detect any motion that disturbs the wave pattern

Capacitance Detector: Emits a magnetic field and monitors the field for disturbances

Closed Circuit Television (CCTV): Uses cameras that can be monitored in real time or can record activity

Lighting Systems

Continuous Lighting: An array of lights that provide an even amount of illumination across an area

Standby Lighting: Illuminates only at a certain time or on a schedule

Movable Lighting: Repositionable as needed

Emergency Lighting: Lighting with exclusive power to function when primary power is not available

Types of Lighting

Fluorescent: Low pressure mercury-vapor gas-discharged lamp using fluorescence to produce visible light

Mercury Vapor: Gas-discharged lamp that uses an electric arc through vaporized mercury to produce light

Sodium Vapor: Gas-discharged lamp that uses sodium in an excited state to produce light

Quartz Lamp: A lamp of an ultraviolet light source, like mercury vapor, contained in a fused-silica bulb that transmits ultraviolet light with little absorption

Additional Perimeter Measures

Patrol Force: Guards can use discriminating judgment that automated systems cannot

Access Control: every successful and unsuccessful attempt to enter the facility should record:

- Date and Time
- Specific Entry Point
- User ID employed during the attempt

Building and Internal Security

Doors

Vault Doors: Leading into walk-ins, safes, or security rooms

Personal Doors: Used by humans to enter the facility

Industrial Doors: Large doors that allow access for larger vehicles

Vehicle Access Doors: Doors to parking facilities or other lots

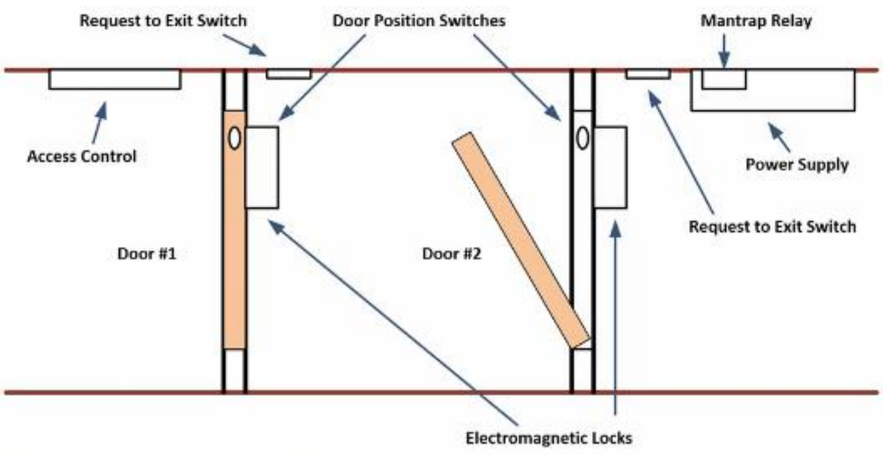
Bullet Resistant Doors: Doors designed to withstand firearms

Electric Locks: a.k.a. cipher locks use a keypad that require a code to open the lock

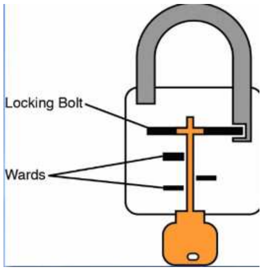
Proximity Authentication Device: uses a programmable card to deliver an access code when in the vicinity of the reader abnd generally include:

- Electromagnetic lock
- Credential reader
- Closed door sensor

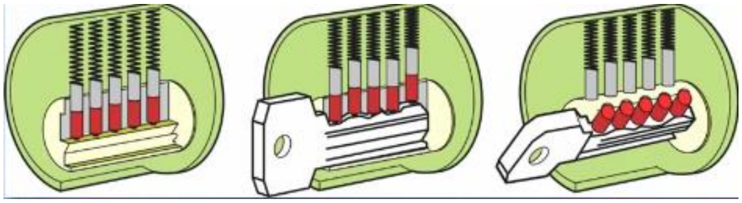
Mantraps:



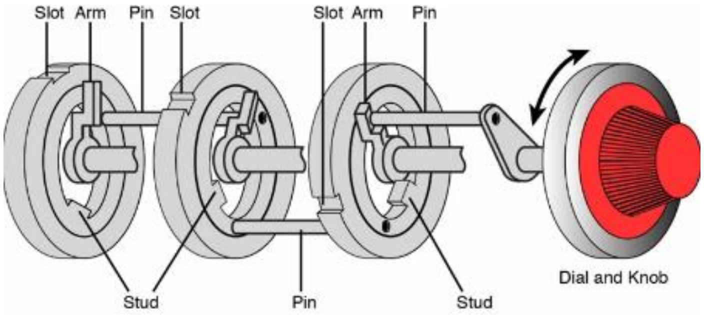
Warded Locks:



Tumbler Locks:



Combination Locks:



Glass Entries

Standard: Used in residential areas and is easily broken

Tempered: Created by heating the glass to give it extra strength

Acrylic: Made of polycarbonate acrylic; much stronger than regular glass but produces toxic fumes when burned

Laminated: 2 sheets of glass with a plastic film to deter breaking

Additional Interior Considerations

Visitor Control: these are ways to accompany a contractor or visitor to their destination

Equipment Rooms: Lock and keep a strict inventory of all equipment to discover theft

Work Areas: Prohibiting some employees from certain areas may be beneficial

Secure Data Centers and Fire Detection Systems

Data Centers

- They should not be located on top floors or in basements
- An off switch should be located near the door for easy access
- Separate HVAC for these rooms is recommended
- Environmental monitoring should be deployed to alert of temperature or humidity problems
- Floors should be raised to help prevent water damage
- All systems should have a UPS with the entire room connected to a generator

Environmental Security and Fire Detection Systems

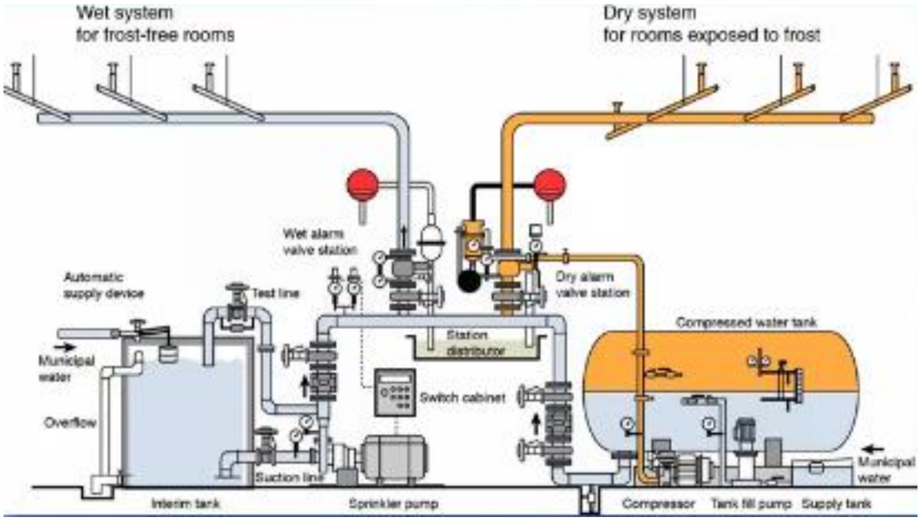
Smoke Activated: This operates using t photoelectric device to detect variations in light caused by smoke particles

Heat Activated/Sensing: This operates by detecting temperature changes either by a predetermined temperature or a rise rate

Flame Actuated: Employs optical devices to 'look at' the protected area; these generally react faster than non-optical devices.

Wet Pipe: This uses water contained in pipes to extinguish the fire. These are not recommended for areas that may freeze or where water may damage equipment

Dry Pipe: This system the water is held in a holding tank



Preaction: This is a dry system where the sprinkler head holds a thermal-fusible link that must melt before water is released. Great for computer rooms

Deluge: This allows large amounts of water to be released into the room.

EPA Approved Halon Replacements

- Water
- Argon
- NAF-S-III
- FM-200

Types of Power Issues

Surge: a prolonged high voltage above normal voltage

Brownout: a prolonged drop in power below normal voltage

Fault: a momentary power outage

Blackout: a prolonged power outage

Sags: a momentary reduction in the level of power

Static Electricity Prevention

- Antistatic spray
- Maintain proper humidity levels
- Use antistatic mats and wristbands

Dirty Power Protection

Power Conditioners: These live between the wall outlet and the device and smooth out the fluctuations of power to protect against sags and surges.

Uninterruptible Power Supply (UPS): These live between the wall outlet and the device and use a battery to provide power when primary power is not available.

HVAC Guidelines

Issues:

- Heat: Excessive heat can cause reboots and crashes
- High Humidity: High humidity causes corrosion
- Low Humidity: Low humidity causes static

Guidelines:

- 100 F affects magnetic media like floppy disks
- 175 F affects computers and peripherals
- 350 F affects paper products

Equipment Security and Personal Security

Equipment

Corporate procedures should address the following issues:

- Tamper Protection
- Encryption
- Inventory
- Physical Protection of Security Devices
- Portable Media Procedures

Personal

Human Resources are the most important assets!

An Occupant Emergency Plan (OEP) provides coordinated procedures for minimizing injury and even loss of life.

Chapter 4 - Security Architecture and Design

Security Model Concepts

Confidentiality
Integrity
Availability
Defense in Depth

System Architecture

The process of describing and representing the components that make up the planned system and the interrelationship between the components.

Answers questions such as:

- What is the purpose of the system?
- Who will use it?
- In what environment, will it operate?

Steps:

1. System Design Phase: System requirements are gathered, and the way the requirements will be met are mapped out.
2. Development Phase: Hardware and software components are assigned to individual teams for development.
3. Maintenance Phase: The system and security architecture are evaluated to ensure that the system operates properly and that the security of the systems is maintained.

ISO/IEC 42010:2011 Terminology

- Architecture: Describes the organization of the systems, including its components and their interrelationships along with the principles that guide its design and evolution.
- Architectural Description (AD): Comprises the set of documents that convey the architecture in a formal manner.
- View: The representation of the system from the perspective of the stakeholder or a set of stakeholders.
- Viewpoint: A template used to develop individual views that establish the audience, techniques, and assumptions made.

Computing Platforms

Mainframe/Thin Clients

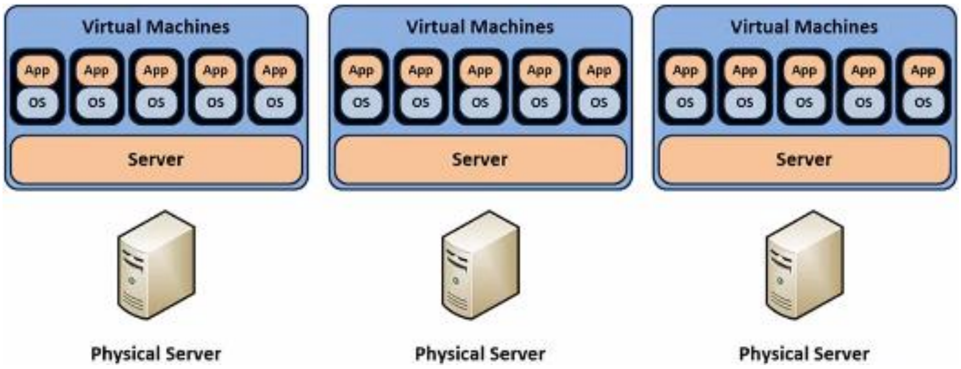
Distributed Systems (Client/Servers)

Middleware

Embedded Systems

Mobile Computing

Virtual Computing



Security Services

Boundary Control: Placing various components in security zones and maintaining boundary control among them

Access Control Services: Gives users only the access they need to do their jobs

Integrity Services: Ensures that data moving through the OS or application can be verified to not have been damages or corrupted

Cryptographic Services: Scrambling or encrypting information in transit

Auditing and Monitoring Services: Method of tracking the activities of the user and od the operations of the system process

System Concepts

CPU

- Executes all the instructions in the code
- Multiprocessing allows the computer to execute multiple instructions in parallel
- CPU's have their own memory
- Can work in user mode or privileged mode.
- If an instruction sent to the CPU is marked to be performed in privileged mode, it must be a trusted OS process and is given functionality not available in user mode.

RAM

Desktop

- SDRAM: Synchronous Dynamic Random Access Memory
- DDR SDRAM: Double Data Rate Synchronous Dynamic Random Access Memory
- DDR2 SDRAM: Double Data Rate Two (2) Synchronous Dynamic Random Access Memory
- DDR3 SDRAM: Double Data Rate Three (3) Synchronous Dynamic Random Access Memory

Laptop

- SODIMM (Small Outline DIMM)

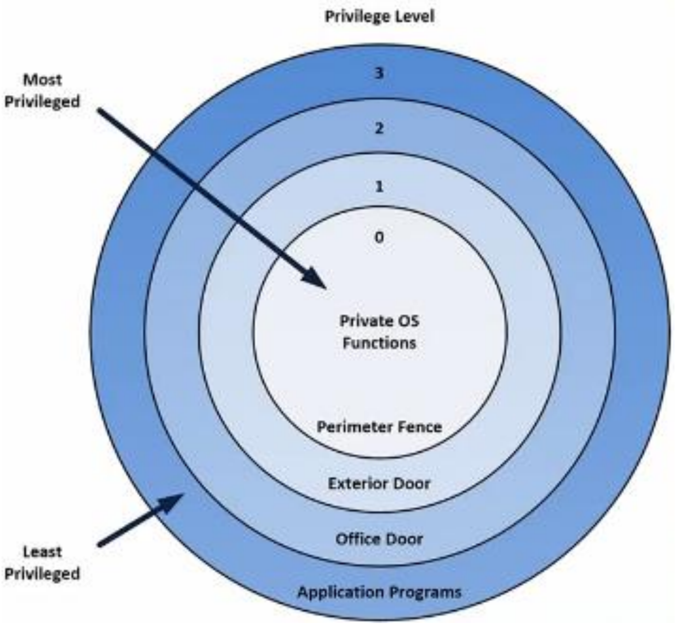
ROM

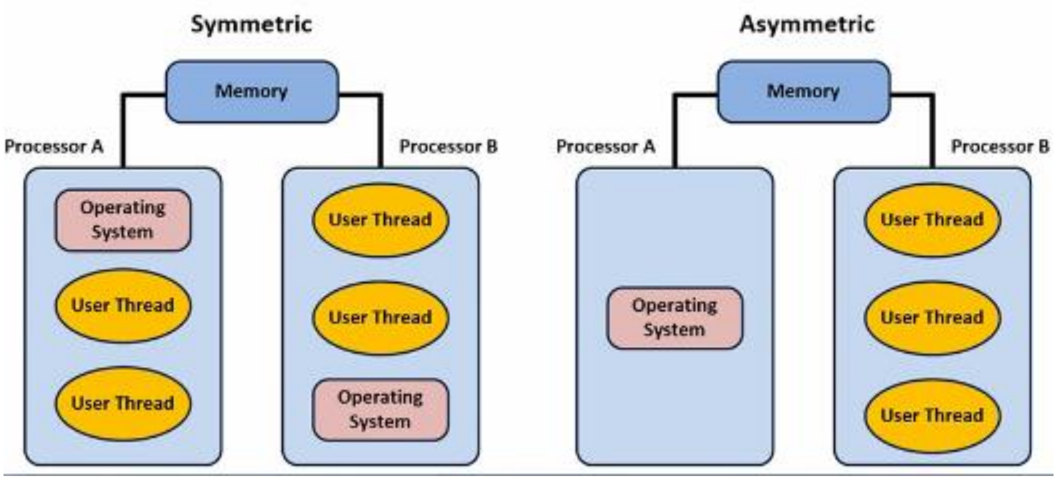
- Flash Memory: A type of electrically programmable ROM
- Programmable Logic Device (PLD): An integrated circuit with connections or internal logic gates that can be changed through a programming process.
- Field Programmable Gate Array (FPGA): A type of PLD that is programmable by blowing fuse connections on the ship or using an antifuse that makes a connection when a high voltage is applied to the junction.
- Firmware: A type of ROM where a program or low-level instructions are installed.

Memory Concepts

- Associative Memory: Searches for a specific data value in memory rather than using a specific memory address.
- Implied Addressing: Refers to registers usually contained inside the CPU.
- Absolute Addressing: Addresses the entire primary memory space. The CPU uses the physical memory addresses that are called absolute addresses.
- Cache: A relatively small amount (compared to primary memory) of high-speed RAM that holds the instructions and data from primary memory and that has a high probability of being accessed again during the currently executing portion of a program.
- Indirect Accessing: The type of memory addressing there the address location specified in the program instruction contains the address of the original desired location.
- Logical Addressing: The address at which a memory cell or storage element appears to reside from the perspective of an executing application program.
- Relative Address: Specifies its location by indications its distance from another address.
- Virtual Memory: A location on the HDD used temporarily for storage when memory space is low.
- Memory Leak: Occurs when a program incorrectly manages memory allocations, which can become exhausted as an application runs.

Enforcing Process Security and Multitasking





Security System Architecture

1. Views the components that comprise the system from a security perspective.
2. Should be derived from the security policy of the organization.
3. System-specific policy that speaks to the level of security required on the device, operating system, or application level that must be more detailed.

Trusteed Computer System Evaluation Criteria (Orange Book Concepts)

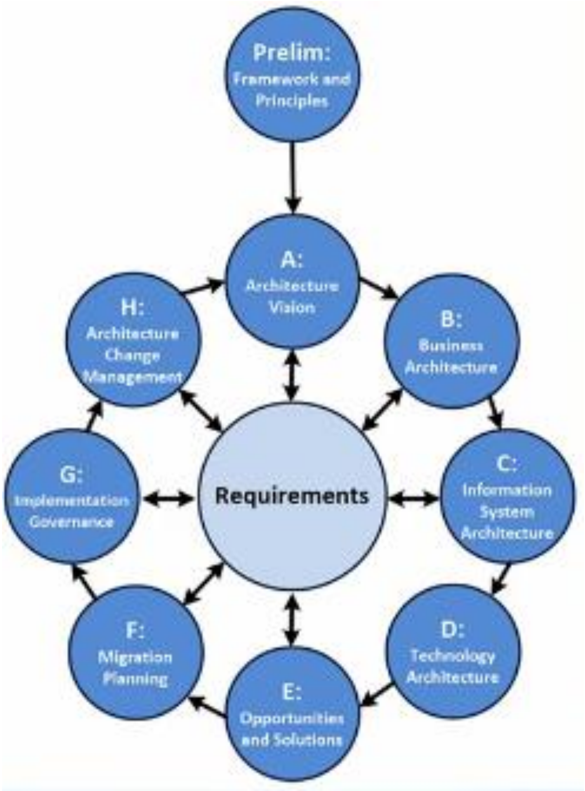
- Trusted Computer Base (TCB): Composed of the components (hardware, firmware, and software) that are trusted to enforce the security policy of the system.
- Security Perimeter: This is the dividing line between the trusted parts of the system and those that are untrusted.
- Reference Monitor: A system component that enforces access controls on an object
- Security Kernel: The hardware, firmware, and software elements of a TCB that implements the reference monitor concept

Security Architecture Frameworks

- Zachman Framework: A two-dimensional model that intersects communication interrogatives (what, why, where, etc.) with various viewpoints (planner, owner, designer, etc.)
- Sherwood Applied Business Security Architecture (SABSA): It also attempts to enhance the communication process between stakeholders
- Information Technology Infrastructure Library (ITIL): Set of best practices, which have become the de facto standard for IT service management

The Open Group Architecture Framework (TOGAF)

Calls for an Architetural Development Method (ADM) that employs an iterative process that calls for individual requirements to be continusously monitored and updated as needed.



Security Architecture Documentation

- ISO/IEC 27000 Series: Establishes information security standards published jointly by the International Organization for Standardization (ISO) and the Electrotechnical Commission (IEC)
- Control Objectives for Information and Related Technology (CobiT): Derived from COSO framework created by the Committee of Sponsoring Organizations of the Treadway Commission and deals with IT Governance.

Security Models and Modes

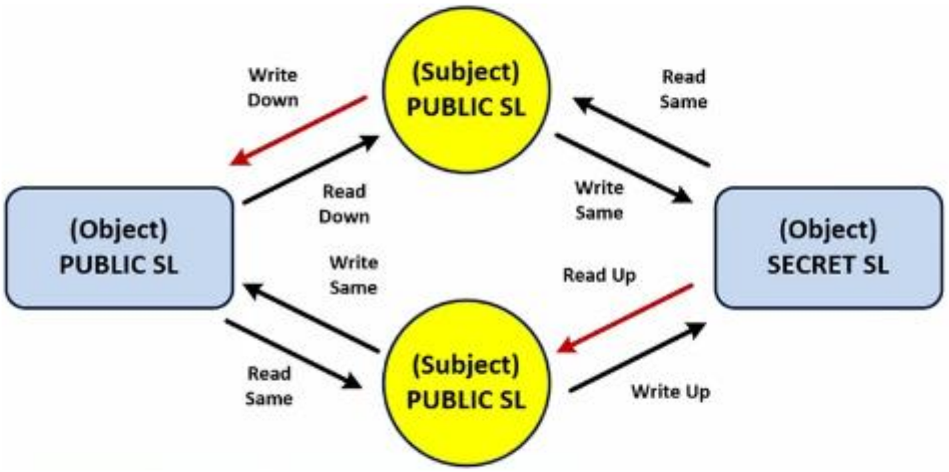
- State Machine Models: Examines every possible state the system could be in and ensures that the system maintains the proper security relationship between objects and subjects in each state.
- Multilevel Lattice Models: Assigns each security subject a security label that defines the upper and lower bounds of the subject’s access to the system. Applies controls to all objects by organizing them into levels or lattices.
- Matrix Based Models: Organizes tables of subjects and objects indicating what actions individual subjects can take upon individual objects; often implemented as a control matrix.
- Noninterference Models: More concerned with a subject’s knowledge of the state of the system at a point in time, it concentrates on preventing the actions that take place at one level from altering the state presented to another level.
- Information Flow Models: Attempts to prevent the flow of information from one entity to another that violates or negates the security policy.

Bell-LaPadula Model

It incorporates three basic rules with respect to the flow of information in a system:

1. The simple security rule: A subject cannot read data located at a higher security level than that possessed by the subject (also called no read up).

2. The * property rule: A subject cannot write to a lower level than that possessed by the subject (a.k.a. no read down or the confinement rule).
3. The strong star property rule: A subject can perform both read and write functions only at the same level possessed by the subject.



Bell-LaPaluda Limitations:

1. It contains no provision or policy for changing data access control. Therefore, it only works well with static systems.
2. It does not address what are called covert channels. A low-level subject can sometimes detect the existence of a high level object when it is denied access. Sometimes is is not enough to hide the content of an object; also their existence might have to be hidden.
3. Its main contribution at the expense of other convepts is confidentiality.

Biba Model

Applies to a series of properties or axioms to guide the protection of integrity:

1. * Integrity Axiom: A subject cannot write to a higher integrity level that that to which s/he has access (no write up).
2. Simple Integrity Axiom: A subject cannot read to a lower integrity level that to which s/he has access (no read down).
3. Invocation Property: A subject cannot invoke (request service) of higher authority.

Clark-Wilson Integrity Model

Describes a series of elements that are used to control the integrity of data

- User: An active agent
- Transformation Procedure (TP): An abstract operation, such as read, write, and modify, implemented through programming
- Constrained Data Item (CDI): An item that can be manipulated only through a TP
- Unconstrained Data Item (UDI): An item that can be manipulated by a user via read and write operations
- Integrity Verification Procedure (IVP): A check of the consistency of data with the real world

Additional Models

- Lipner Model: An implementation that combines the elements of Bell-LaPadula and the Biba models.

- Brewer-Nash (Chinese Wall) Model: Introduced the concept of allowing access controls to change dynamically based on a user's previous actions
- Graham-Denning Model: Attempts to address an issue ignored by the Bell-Paludal and Biba models. It deals with the delegate and transfer rights.
- Harrison-Ruzzo-Ullman Model: Restricts the set of operations that can be performed on an object to a finite set to ensure integrity.

Security Modes

- Dedicated Security Mode: Employs a single classification level. All users can access all data, but they must sign an NDA and be formally approved for access on a need-to-know basis.
- System High Security Mode: All users have the same security clearance but they do not all possess a need-to-know clearance for all the information in the system.
- Compartmented Security Mode: All users must possess the high security clearance, but they must also have valid need-to-know clearance, an NDA, and formal approval for all information to which they have access.
- Multilevel Security Mode: System allows two or more classification levels of information to be processed at the same time.

System Evaluation and Assurance Levels

1. Trusted Computer System Evaluation Criteria (TCSEC): This was developed but he National Computer Security Center (NCSC) for the U.S. DoD to evaluate products.
2. Orange Book: A collection of criteria based on the Bell-LaPadula model used to grade or rate the security offered by a computer system product.
3. Red Book: This is like the Orange Book but addresses network security.
4. ITSEC: This addresses integrity and availability as well as confidentiality; mainly a set of guidelines used in Europe.
5. Common Criteria: Uses Evaluation Assurance levels (EALs) to rate systems with each representing a successively higher level of security testing and design in a system.
6. TSEC Classes:
   a. D: Minimal Protection
   b. C: Discretionary Protection
      i. C1: Discretionary Security Protection
      ii. C2: Controlled Access Protection
   c. B: Mandatory Protection
      i. B1: Labeled Security Protection
      ii. B2: Structured Protection
      iii. B3: Security Domains
   d. A: Verified Protection
      i. A1: Verified Design

ITSEC Ratings

1. 10 classes, F1 to F10, evaluate the functional requirements
2. 7 classes, E0 to E6, evaluate assurance requirements

Common Criteria Assurance Levels

1. EAL1: Functionally tested
2. EAL2: Structurally tested
3. EAL3: Methodically tested and checked
4. EAL4: Methodically designed, tested, and reviewed
5. EAL5: Semi-formally designed and tested
6. EAL6: Semi-formally verified design and tested
7. EAL7: Formally verified designed and tested

Common Criteria

This uses a concept called a protection profile during the evaluation process. A protection profile contains the following elements:

- Descriptive Elements
- Rationale
- Functional Requirements
- Development assurance requirements
- Evaluation assurance requirements

Certification and Accreditation

Certification evaluated the technical system components.

Accreditation occurs when the adequacy of a system’s overall security is accepted by management

NIACAP Accreditation Process:

1. Phase 1: Definition
2. Phase 2: Verification
3. Phase 3: Validation
4. Phase 4: Post Accreditation

Types of Accreditation

1. Type Accreditation: This evaluates an application or system distributed to many different locations.
2. System Accreditation: This evaluates an application or support system.
3. Site Accreditation: This evaluates the application or system at a specific self-contained location.

Security Architecture Threats

1. Maintenance Hooks: A set of instructions built into the code that allow someone who knows about a back door to use the instructions to connect to view and edit the code without using the normal access controls.
2. Time-of-Check (Time-of-Use) attacks: These are attempts to take advantage of the sequence of events that occur as the system completes common tasks.
3. Web based attacks: These operate by making at least one normal request or a modified request aimed at taking advantage of the inadequate input validation and parameters or instruction spoofing.
4. Server based attacks: These attacks focus on the operations of the server OS itself.

Concerns with XML

Security Assertion Markup Language (SAML): This is an XML-based open standard data format for exchanging authentication and authorization data between parties, commonly, between an identity provider and a service provider.

Open Web Application Security Project (OWASP): This is an open-source application security project. This group creates guidelines, testing procedures, and tools to assist with web security. They are also known for maintaining a top ten list of all web application security risks.

Database Security and Distributed System Security

1. Inference: Occurs when someone has access to information at one level that allows them to infer information at or about another level.
2. Polyinstantiation: The main mitigation technique for inference; the development of a detailed version of an object from another object using different values in the new object.
3. Aggregation: Assembling information units at one sensitivity level and having the resultant totality of data being of a higher sensitivity level than the individual components.
4. Contamination: The intermingling or mixing of data of one sensitivity or need-to-know level with that of another level.

Data Mining Warehouse

A repository of information from heterogeneous databases

Allows for multiple sources of data to not only be stored in one place, but also to be organized in such a way that redundancy of data is reduced (normalization)

Data mining tools are used to manipulate the data to discover relationships that may not have been apparent before.

Distributed Systems Security

Special cases in which additional security concerns might be warranted:

1. Cloud Computing: This is the centralization of data in a web environment that can be accessed from anywhere at any time.
2. Grid Computing: This is the process of harnessing the CPU power of multiple physical machines to perform a job.
3. Peer to Peer Computing: This is any client-server solution in which any platform may act as a client, server, or both.

Chapter 5 – Access Control

Access Control Concepts

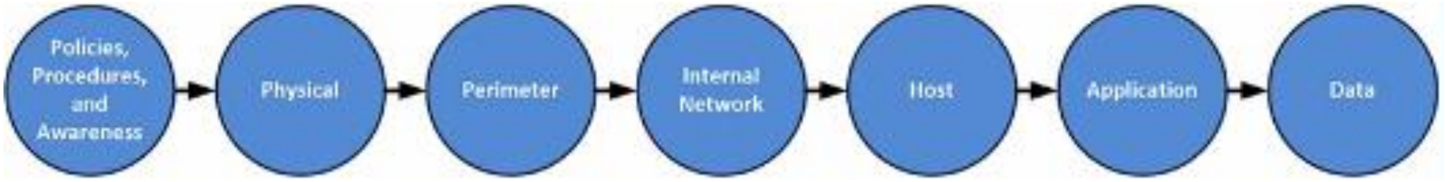
- CIA Triad: Confidentiality, Integrity, and Availability
- Confidentiality: This prevents the disclosure of data or information to unauthorized entities. (Ant. disclosure)
- Integrity: This ensures that data is protected from unauthorized modifications or data corruption. (Ant. corruption)
- Availability: This ensures that data is accessible when and where it is needed. (Ant. destruction, isolation)

Default Stance

- For a default stance, organizations must choose between an allow-by-default or deny-by-default stance
- An allow-by-default stance permits access to any data unless a need exists to restrict access
- The deny-by-default stance is much stricter because it denies any access that is not explicitly permitted

Defense in Depth

- A defense-in-depth strategy refers to the practice of using multiple layers of security between data and the resources on which it resides and possible attackers.



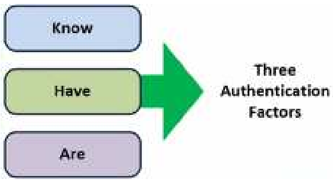
1. Identify Resources
   a. Which resources need to be protected?
   b. How are the resources accessed?
   c. Which data on the resources will be accessed?
   d. Who will be accessing the data?
2. Identify Users
   a. Document user levels and needs
   b. Analyze needs against organizational policies, legal issues, data sensitivity, and risk.
3. Identify the relationships between the resources and the users

Identification and Authentication

- Identification is the act of a user professing an identity to an access control system. The most common form of identification is a user ID or username.
- Authentication is the act of validating a user with a unique identifier by providing the appropriate credentials. The most common authentication method is a password.

Three Factors for Authentication

Three factor authentication ensures that a user provides three factors. An example of three factor authentication would be providing a username, password, smart card, and fingerprint at login. For login to be considered strong authentication, u user must provide factors from at least two different categories.



- Knowledge factor authentication: Something a person knows
- Ownership factor authentication: Something a person has or possesses
- Characteristic factor authentication: Something a person is

Type I authentication factors

- Most popular form of authentication used by this category is password authentication
- Other knowledge factors include date of birth, mother's maiden name, key combination (or PIN).
- If knowledge factor authentication is used, identify/account and password management are crucial.

Elements of proper account management include the folllowing:

- Establish a formal process for establishing, issuing, and closing user accounts.
- Periodically review user accounts.
- Implement a process for tracking access authorization.
- Periodically rescreen personnel in sensitive positions.
- Periodically verify the legitimacy of user accounts.

User account reviews can be performed on an enterprise wide, system wide, or application-by-application basis.

Password Types and Management

Standard Word or Simple Passwords: Consist of a single word that often includes a mixture of upper and lowercase letters.

Combination Passwords or Composition Passwords: Uses a mix of dictionary words, usually two unrelated words.

Static Passwords: Remains the same for each login. Most often seen in peer-to-peer networks.

Complex Passwords: Includes a mixture of upper and lower case letters, numbers, and special characters.

Passphrase Passwords: Requires that a long phrase be used.

Cognitive Passwords: A piece of information that can be used to berify an individuals identity. This information is provided to the system by answering a series of questions based on the user's life, such as favorite color, pet's name, mother's maiden name, and so on.

One-Time-Passwords or Dynamic Passwords: Only used once to log in to the access control system

Graphical Passwords (CAPCHA): Uses graphics as a part of the authentication mechanism.

Numeric Passwords: Includes only numbers and is easily guessed because of known possibilities.

Password Policies

- Password Life: How long the password will be valid.
- Password History: How long before a password can be reused.
- Authentication Period: How long a user can remain logged in.
- Password Complexity: Password structure
- Password Length: Password length in characters.

Password Types and Management

Operating System Password Management

- UNIX
  - /etc/passwd and /etc/shadow file
  - root account
- Windows
  - C:\windows\system32\config\SAM
  - Administrator accounts
  - Guest accounts

Ownership Factors

- Type II authentication factor
- Ownership factors can include token devices, memory cards, and smart cards
  - Synchronous token generates a unique password at fixed time intervals with the authentication server.
  - Asynchronous token generates the password based on a challenge/response technique with the authentication server, with the token device providing the correct answer to the authentication server's challenge.
  - Memory Card is a swipe card that is issued to valid users. The card contains user authentication information. When the card is swiped through a card reader, the information stored on the card is compared to the information that the user enters.
  - Smart Cards or Integrated Circuit Cards(ICC): contain memory but also contain a chip like bank or credit cards.
    - Contact Cards require physical contact with the reader, usually swiping.
    - Contactless Cards or Proximity Cards simply need to be in proximity to the reader.
    - Hybrid Cards are available that allow a card to be used in both contact and contactless systems.

Ownership Character Physiological Behavioral Factors

Characteristic Factors

- Type III authentication factor
- Biometric technology allows the user to be authenticated based on physiological behavior or characteristics.
  - Physiological Characteristics include any unique physical attribute of the user including, iris, retina, and fingerprints
  - Behavioral Characteristics measure a person's actions in a situation including voice patters and data entry characteristics.

Physiological Characteristic Factors

- Fingerprint: scans the ridges of a finger

- Fingerprint Scan: Extracts only certain features from a fingerprint.
- Hand Geometry: Obtains size, shape, bone length, finger length, or other layout attributes of a user's hand.
- Hand Topography: Records peaks, valleys, and shape of the hand.
- Palm or Hand Scan: Combines fingerprint and hand geometry.
- Facial Scan: Records facial characteristics including bone structure, eye width, and forehead size.
- Retina Scan: Scans the retina's blood vessel pattern.
- Iris Scan: Scans the colored portion of the eye including all rifts, coronas, and furrows.
- Vascular Scans: Scans the pattern of the veins in the users hand or face.

Behavioral Characteristic Factors

- Signature Dynamics: Measures stroke speed, pen pressure, and acceleration while the user writes a signature.
- Keystroke Dynamics: Measures the typing pattern that a user uses when inputting a password or other predetermined phrase.
- Voice Pattern or Print: Measures the sound pattern of a user stating a certain word.

Biometric Considerations

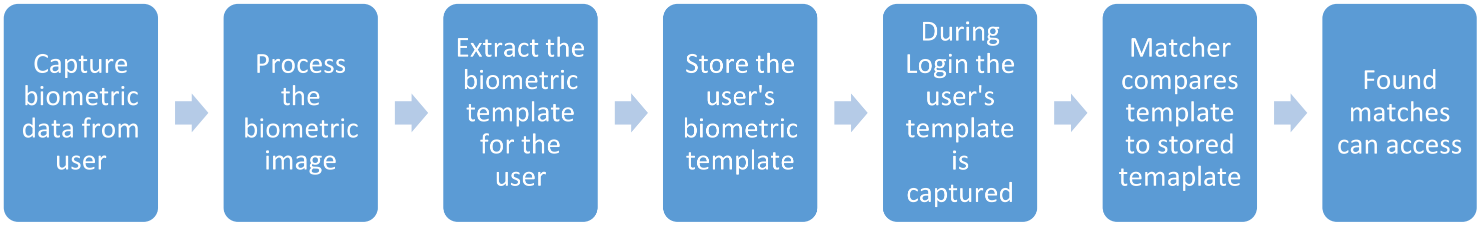
- Enrollment Time: The process of obtaining the sample that is used by the biometric system.
- Feature Extraction: The approach to obtaining the information from a collected sample of a user's characteristics.
- Accuracy: The most important characteristic; it is how correct the overall readings will be.
- Throughput Rate: The rate at which the system can scam and complete the analysis to permit or deny access.
- Acceptability: Describes the likelihood that users will accept and follow the system.
- False Rejection Rate (FRR): A measurement of the percentage of valid users that will be falsely rejected.
- False Acceptance Rate(FAR): A measurement of the percentage invalid users that will be falsely accepted.
- Crossover Error Rate (CER): the point at which FRR equals FAR. This is expressed as a percentage and most important.

Biometric Methods ranked by effectiveness:

1. Iris Scan
2. Retina Scan
3. Fingerprint
4. Handprint
5. Hand Geometry
6. Voice Pattern
7. Keystroke Pattern
8. Signature Dynamics

Biometric Methods ranked by user acceptance:

1. Iris Scan
2. Voice Pattern
3. Keystroke Pattern
4. Signature Dynamics
5. Hand Geometry
6. Hand Print
7. Fingerprint
8. Iris Scan
9. Retina Scan

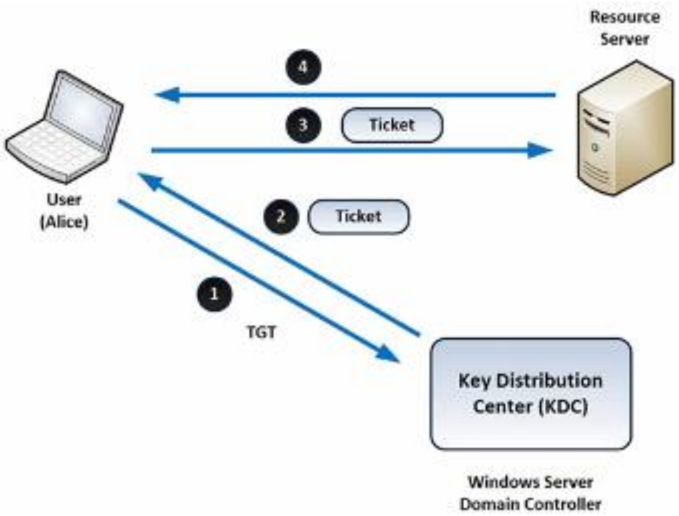

Capture biometric data from user
Process the biometric image
Extract the biometric template for the user
Store the user's biometric template
During Login the user's template is captured
Matcher compares template to stored temaplate
Found matches can access

Authorization Concepts

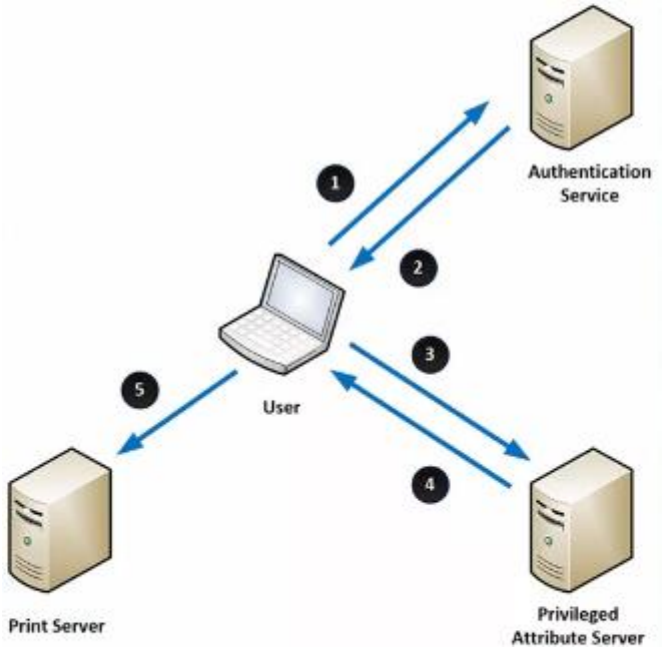
Access Control Policy defines the method for identifying and authenticating users and the level of access that is granted to users

Separation of Duties prevents fraud by distributing tasks and their associated rights and privileges between more than one user.

- Dual Controls: two or more users are authorized and required to perform certain functions
- Split Knowledge: ensures that no single user has all the information to perform a task.
- Principle of Least Privilege: requires that a user or process is given only the minimum access privilege needed to perform a task.
- Need-to-Know: principle defines what the minimums for each job and function are.
- No Access: The recommended default level. This means that if nothing was specifically allowed, then the user or group cannot access the resource.
- Directory Service: is a database designed to centralize data management regarding network subjects and objects.
  - X.500
  - Lightweight Directory Access Protocol (LDAP)
  - X.400
- Single Sign-On (SSO): is when a user enters login credentials once and can access all resources in the network.
  - SSO comes in Kerberos and SESAME
- Kerberos: is an authentication protocol that uses a client/server model. Used in Windows, Apple, SUN, and Linux.
  - Symmetric Key Cryptography and provides integrity and confidentiality
  - Key Distribution Center (KDC) is the repository for all users and service secret keys.
  - Secure European System for Applications in a Multivendor Environment (SESAME)


Resource Server
4
3
Ticket
User (Alice)
2
Ticket
1
TGT
Key Distribution Center (KDC)
Windows Server Domain Controller

- SESAME: Secure European System for Applications in a Multi-Vendor Environment extended Kerberos' to address weaknesses
  - Uses both symmetric and asymmetric cryptography to protect interchanged data
  - Uses Privileged Attribute Certificates (PAC's) instead of tickets.
  - Uses two certificates: One for authentication and another defines the privilege.
  - The trusted authentication server is referred to as the Privileged Attribute Server (PAS), which performs roles like KDC in Kerberos.
  - SESAME can be incorporated into Kerberos.



Authorization Concepts

- Security domain is a set of resources that follow the same security policies and are available to a subject.
- Domains are usually arranged in a hierarchical structure of parent and child domains.

Federated Identity

- Each organization that joins the federation agrees to enforce a common set of policies and standards.
- Uses two basic models for linking organizations within the federation
  - Cross-Certification Model: each organization certifies that every other organization is trusted. Each organization must verify and certify through due diligence that the other organizations meet or exceed standards.
  - Trusted Third-Party or Bridge Model: each organization subscribes to the standards of a third party. The third party manages verification, certification, and due diligence for all organizations.

User Accountability

Accountability: the organization's capability to hold users responsible for the actions they perform.

Accountability usually involves the following:

- Auditing and Reporting
- Vulnerability Assessment
- Penetration Testing
- Threat Modeling

Auditing and Reporting: Ensures that users are held accountable for their actions, but an auditing mechanism can repot only on events that it is configured to monitor.

You should monitor the following events:

- Network Events
- System Events
- Application Events
- User Events
- Keystroke Activity

Keep in mind that any auditing activity will impact the performance of the system being monitored.

Auditing Guidelines:

- Develop an audit log management plan that includes mechanisms to control the log size, backup process, and periodic review plans.
- Ensure that the ability to delete an audit log file is a two-person control that requires the cooperation of at least two administrators.
- Monitor all high-privilege accounts (including all root users and administrative-level accounts)
- Ensure that the audit trail includes who processed the transaction, when the transaction occurred (date/time), where the transaction occurred (which system), and whether the transaction was successful or not.
- Ensure that deleting the log and deleting data within the log cannot occur unless the user has the appropriate administrative-level permissions.
- To identify abnormal patterns of behavior, you should first identify normal patterns of behavior.
- Also, you should establish the clipping level, which is a baseline of user errors above which violations will be recorded.
- Audit trails must be monitored, and automatic notifications should be configured.

Vulnerability Assessment

Vulnerability Assessments usually fall into one of three categories:

- Personnel Testing: Reviews standard practices and procedures that users follow.
- Physical Testing: Reviews facility and perimeter protections.
- System and Network Testing: Reviews systems, devices, and network topology.

The security analyst that performs the vulnerability assessment must understand the system and devices that are on the network and the job they perform.

Penetration Testing and Threat Modeling

Goal is to simulate an attach to identify any threats that can stem from internal or external resources that plan to exploit the vulnerabilities of a system or device.

Steps include:

1. Document information about the target system or device.
2. Gather information about attack methods against the target system or device. This includes doing port scans.
3. Identify the known vulnerabilities of the target system or device.
4. Execute attacks against the target system or device to gain user and privileged access.
5. Document the results of the penetration test, and report the findings to management with suggestions for remedial action.

Penetration Test Types:

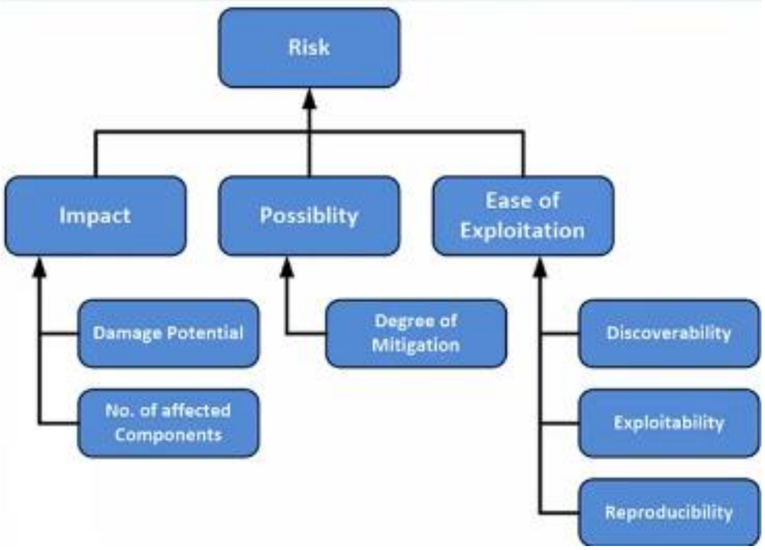
- Blind Test: The testing team is given limited knowledge of the network using publicly avilable information. The organization's security team knows that an attack is coming. This requires more effort by the testing team, and the testing team must simulate an actual attack.
- Double-Blind Test: This test is like a blind test except the organixzation's security team does NOT know that an attack is coming. Only a few individuals at the organization know about the attack, and they do not share this information with the security team. This test usually requires equal effort for both the testing team and the organization's security team.
- Target Test: Both the testing team and the organization's security team are given maximum information about the network and the type of test that will occur. This is the easiest to complete but will not provide a full picture of the organization's security.

Penetration Strategies

- Zero-Knowledge Test: The testing team is provided no knowledge regarding the organization's network. Testing team can use any means at their disposal to obtain information about the network. This is also called Closed or Black Box Testing.
- Partial Knowledge Test: The testing team is provided with public knowledge regarding the organization's network. Boundaries must be set for this type of test.
- Full Knowledge Test: The testing team is provided with all available knowledge regarding the organization's network. This test is focused more on what attacks can be carried out.

Threat Modeling

Threat Modeling allows you to apply a structured approach to security and to address the top threats that have the greatest potential impact to your application first. It is synonomous with Risk Management.



Access Control Categories

Access Control mechanisms you can use are divided into seven main categories:

1. Compensative: Acts as a mitigation to risk. Ex. include requiring two authorized signatures to release sensitive or confidential information and requiring two keys owned by different people to open a safe deposit box.
2. Corrective: Reduces the effect of an attack or other undesirable event. Ex. installing extinguishers, isolating or terminating a connection, installing firewall rules, and using server images to restore to a previous state.
3. Detective: Detects an attack while it is occurring to alert appropriate personel. Ex. Motion detectors, intrusion detection systems (IDS), logs, guards, investigations, and job rotation.
4. Deterrent: Deters or discourages an attacker. Deter controls often trigger preventative and corrective controls. Ex. User identification and authentication, fences, lighting, and organizational security policies like NDA's
5. Directive: Specifies acceptable practice within an organization. The most popular is an Acceptable Use Policy (AUP)
6. Preventative: Prevents an attack. Ex. Locks, badges, biometric systems, encryption, IPS, security guards, passwords, and security awareness training.
7. Recovery: Recovers a system or device after an attack. Ex. Disaster recovery plans, data backups, offsite facilities.

Any access control that you can implement can fit into one or more access control categories.

Access Control Types:

- Administrative Controls: Implemented to administer the organizations assets and personnel Ex. Personnel Control, data classification, data labeling, security awareness training, and supervision.
- Logical (Technical) Controls: Used to restrict access. Ex. Firewalls, IDS's, IPS's, encryption, authentication systems, protocols, auditing and monitoring, biometrics, smart cards, and passwords.
- Physical Controls: Protect organization's facilities and personnel. Ex. Perimeter security, badges, swipe cards, guards, dogs, man traps, biometrics, and cabling.

Access Control Models

Access control models and concepts that you need to understand include the following:

- Discretionary Access Control: the owner of the objects specified switch subjects can access the resource. The access is based on the subject's identity, profile, or role. DAC is a need-to-know control.

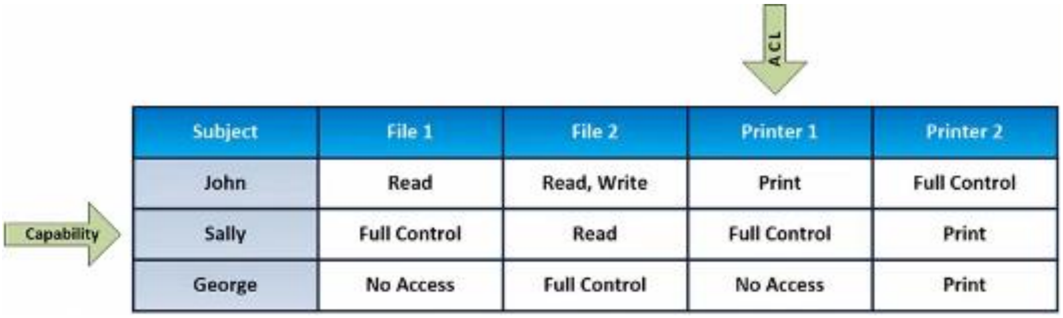
- Mandatory Access Control: Subject authorization is based on security labels. MAC has often described as prohibitive because it is based on a security label system. Under MAC all that is not expressly permitted is forbidden. Only administrators can change the catreory of a reource.
- Role Based Access Control: Each subject assigned to one or more roles. Roles are hierarchical. Access control is defined based on the roles. It can be used to easily enforce minimum privileges for subjects.
- Rule Based Access Control: This facilitates frequent changes to data permissions. Using this method, a security policy is based on global rules imposed for all users.
- Content Dependent Access Control: This makes access decisions based on the data contained within the object.
- Context Dependent Access Control: This is based on subject or object attributes or environmental characteristics. These characteristics can include location or time of day.

Access Control Matrix

Access Control Matrix: This is a table that consists of a list of subjects, a list of onjects, and a list of the actions that a subject can take upon each object. The rows in the matrix are the subjects and the coloumns are the objects.

Common implementations:

- Capabilities Table: A capability corresponds to a subject’s row from an access control matrix. A capability table lists the access rights that a subject has to objects. A capability table is about the subject.
- Access Control List: An ACL corresponds to an object’s column from an access control matrix. An ACL lists all the access rights that subjects have to a particular object, An ACL is about the object.


ACL
Capability

Subject	File 1	File 2	Printer 1	Printer 2
John	Read	Read, Write	Print	Full Control
Sally	Full Control	Read	Full Control	Print
George	No Access	Full Control	No Access	Print

Access Control Administration

Access Control Administration occurs in two basic manners:

- Centralized: A central department or personal oversee the access for all organizational resources. This method ensures that user access is controlled in a consistent manner across the enterprise.
- Decentralized: Personnel closest to the resources, such as department managers and data owners, oversee the access control for individual resources. This method ensures that those who know the data control the access rights to it.

Provisioning Life Cycle

- A formal process for creating, changing, and removing users. This process includes user approval, user creation, user creation standards, and authorization.
- Users should sign a written statement that explains the access conditions, including user responsibilities.
- Access modification and removal procedures should be documented
- User provision policies should be integrated as part of HR management. HR formally requests the creation or deletion of a user account when personnel are hired or terminated.

Access Control Monitoring

- IDS: a system responsible for detecting unauthorized access or attacks against systems and networks.
- IPS: a system responsible for preventing attacks. When an attack begins, an IPS takes actions to prevent and contain the attack.
- Network Based IDS: is the most common IDS and monitors network traffic on a local network segment. An NIDS is affected by a switched network because generally an NIDS monitors only a single network segment.
- Host Based IDS monitors traffic on a single system. Its primary responsibility is to protect the system on which it is installed by using information from the operating system audit trails and system logs.

IDS Implementations

- Signature Based: Analyzes traffic and compares it to attack or state patterns (called signatures) which reside within the IDS database.
- Anomaly Based: Analyzes traffic and compares it to noraml traddic to determin whether said traffic is a threat.
- Rule or Heuristic Based: An expert system that uses a knowlodge base, inference engine, and rule based programming. The knowledge is configured as rules. The data and traffic is analyzed and the rules are applied to the analyzed traffic.

Signature Based Implementations

- Pattern Matching: Compares traffic to a database of attack patterns.
- Stateful Matching: records the initial operating system state. Any changes to the system state that specifically violate the defined rules result in an alert or notification being sent.

Anonaly Based Implementations

- Statistical Anomaly Based: Samples the live environment to record activities. The londer the IDS is in operation the more accurate a profile that will be built.
- Protocol Anomaly Based: Has knowledge of the protocols that it monitors. A profile of normal usage is built and compared to activity.
- Traffic Anomaly Based: The IDS tracks traffic pattern changes. All future traffic patters are compared to the sample.

Access Control Threats

Password Threats

- Dictionary Attack: Occurs when attackers use a dictionary of common words to discover passwords.
- Brute Force or Exhaustive Attack: Works through all possible combinations of numbers and characters.

Social Engineering Threats

Social Engineering Threats: occur when attackers use believable language and user gullibility.

- Phishing: is an attack in which attackers try to learn personal information, including cc and financial data by implementing a fake website that very closely resembles a legitimate website.
- Pharming: pollutes the contents of a computers DNS cache so that requests to a legitimate site are routed to an alternative site.
- Shoulder Surfing: When an attacker watches when a user enters login or other confidential data.
- Identity Theft: When someone obtains personal information, including driver's license number, bank account number, and SSN, and uses that information to assume an identify of the individual whose information was stolen.
- Dumpster Diving: When attackers examine garbage contents to obtain confidential information.
- DoD/DDoS: A DoS attack occurs when attackers flood a device with enough requests to degrade the performance of a targeted service. Some popular DoS attacks include SYN flood attacks and teardrop attacks.

- Buffer Overflow: Buffers are portions of system memory that are used to store information. A buffer overflow occurs when the amount of data that is submitted to the application is larger that the buffer can handle.
- Mobile Code: Any software that is transmitted across a network to be executed on a local system. Malicious mobile code is often used to bypass access control systems.

Malicious Software:

- Virus: Any malware that attaches itself to another application to replicate or distribute itself.
- Worm: Any malware that replicates itself, meaning that it does not need another application or human interaction to propagate.
- Trojan Horse: Any malware that disguises itself as a needed application while carrying out malicious actions.
- Spyware: Any malware that collects private user data, including browser history or keyboard activity.
- Spoofing or Masquerading: occurs when communication from an attacker appears to come from trusted sources. The goal of this type of attack is to obtain access to credentials or other personal information.
- Sniffing or Eavesdropping: occurs when an attacker inserts a device or software into the communication medium that collects all the information transmitted over the medium. Network sniffers are used by both legitimate security professionals and attackers.
- Emanating: Emanations are electromagnetic signals that are emitted by an electronic device. Attackers can target certain devices or transmission mediums to eavesdrop on communication without having physical access to the device or medium. The TEMPEST program, initiated by the US and UK, researches ways to limit emanations and standardizes technologies used.
- Backdoor or Trapdoor: A mechanism implemented in many devices or applications that gives the user who uses the backdoor unlimited access to the device or application.

Chapter 6 - Software Development Security

System Development Life Cycle

1. Initiate
2. Acquire/Develop
3. Implement
4. Operate/Maintain
5. Dispose

1. Gather Requirements
2. Design
3. Develop
4. Release/Maintain
5. Change Management and Configuration Management

Testing and Validation

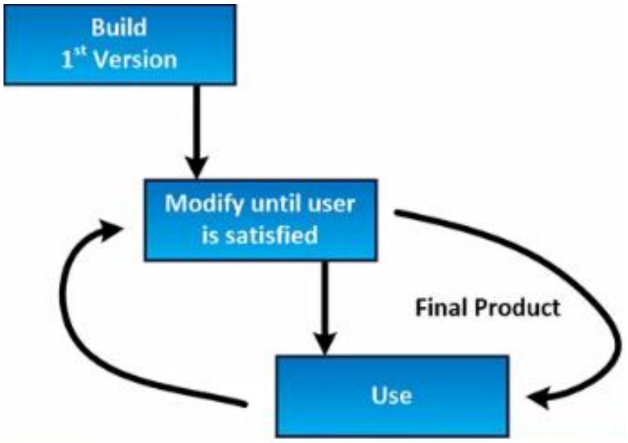
- Verification Testing: Determines whether the original design specifications have been met
- Validation Testing: Takes a higher-level view and determines whether the original purpose of the software has been achieved.
- Integration Testing: Assess the way in which modules work together and determines whether functional and security specifications have been met.
- Acceptance Testing: Ensures that the customer is satisfied with the functionality of the software.
- Regression Testing: Takes place after changes are made to the code to ensure they have neither reduced function or security.

Software Development Security Best Practices

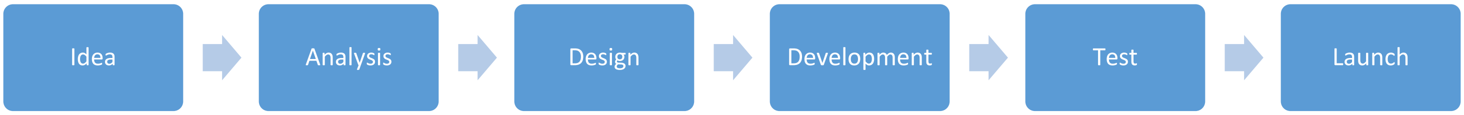
- WASC Web Application Security Consortium is an organization that provides best practices for web based applications.
- OWASP Open Web Application Security Project is another group that monitors web attacks.
- BSI The Build Security In initiative promotes a process-agnostic approach that makes security recommendations with regard to architectures, testing methods, code reviews, and management processes.
- IEC International Electro technical Commission created the 27034 standard, which is part of a larger body of standards called the ISO/IEC 27000 series. These standards provide guidance to organizations in integrating security into the development and maintenance of software applications.

Software Development Methods

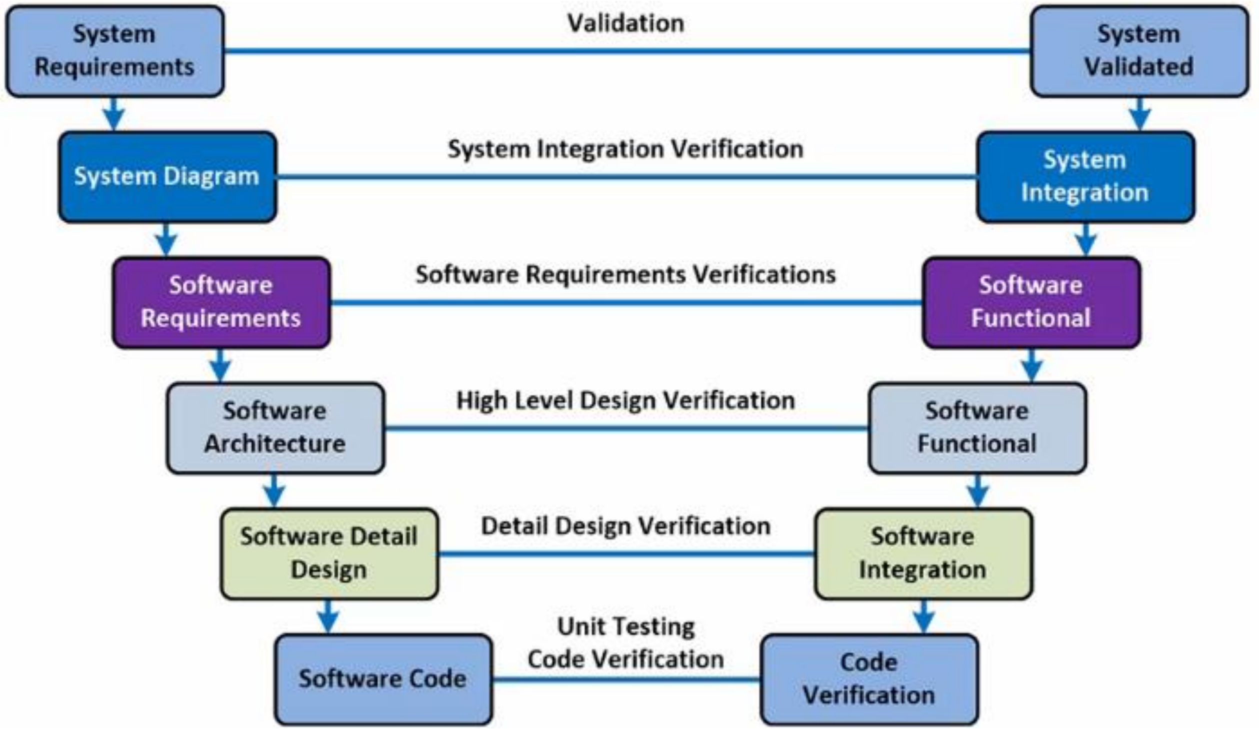
Build and Fix Approach: Describes a method that although certainly used in the past has been largely discredited and is now used as a template for how not to manage a development project.



Waterfall

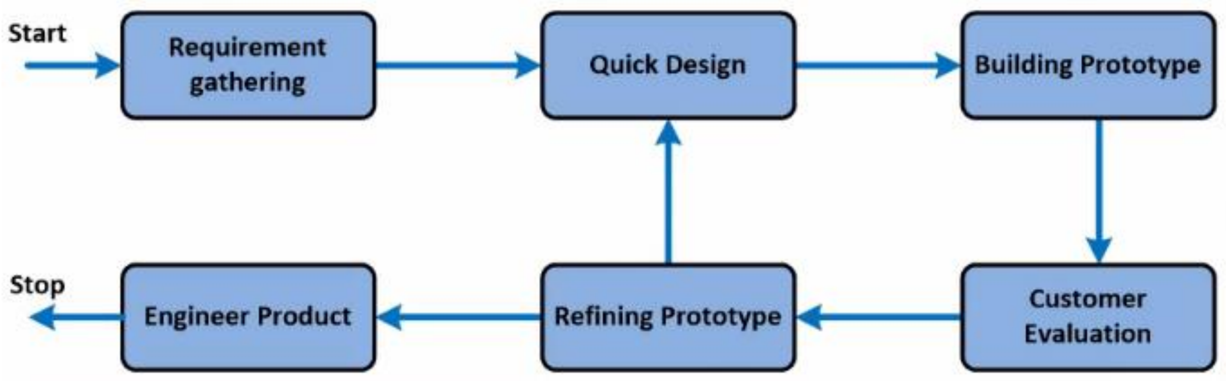


V-Shaped

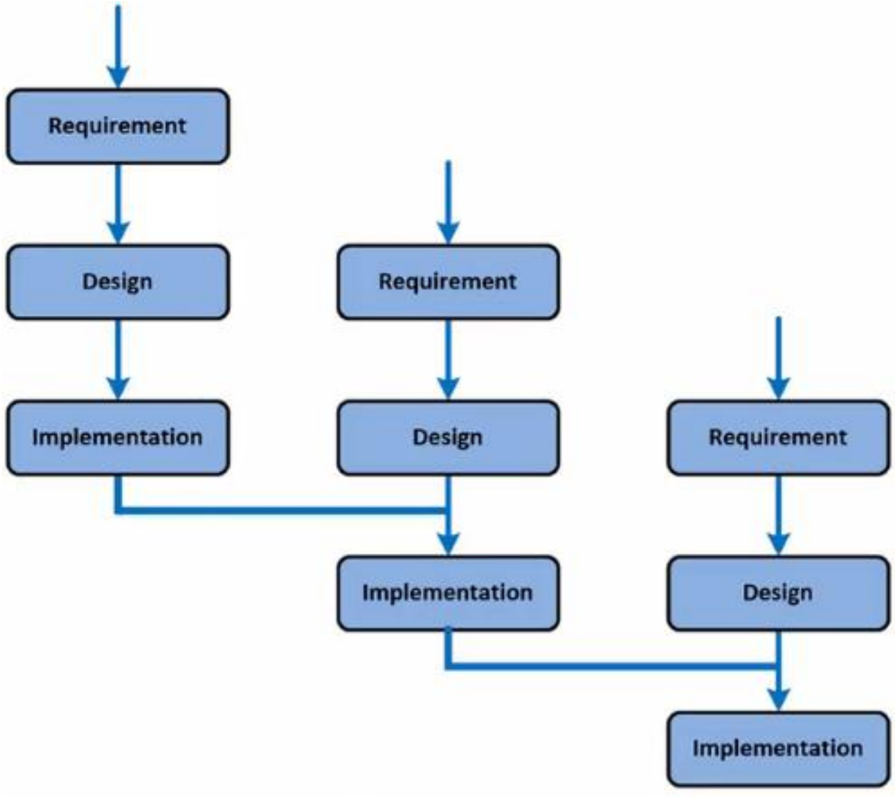


Prototyping

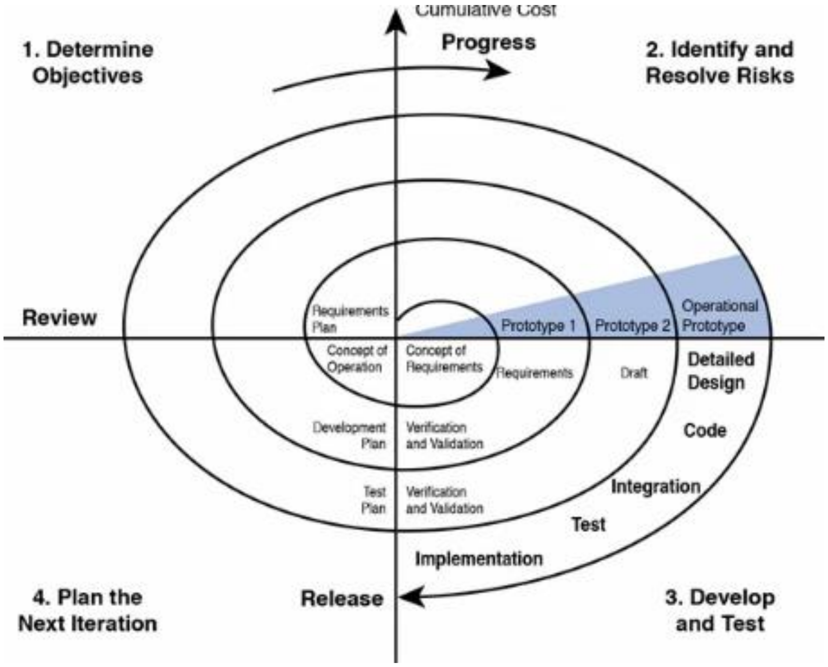
The use of a sample of code to explore a specific approach to solving a problem before extensive time and cost have been invested in the approach.



Incremental



Spiral Model



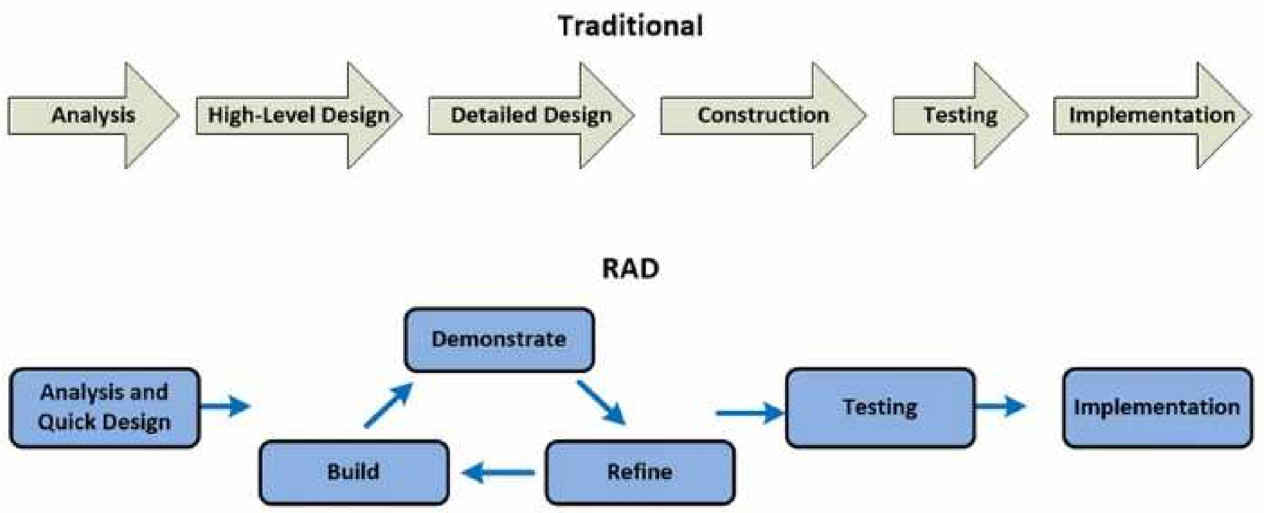
RAD: Rapid Application Development Model: Less time is spent up front on design while emphasis is placed on rapidly producing prototypes with the assumption that crucial knowledge can be gained only through trial and error.

Agile Model: Puts more emphasis on continuous feedback and cross-functional teamwork.

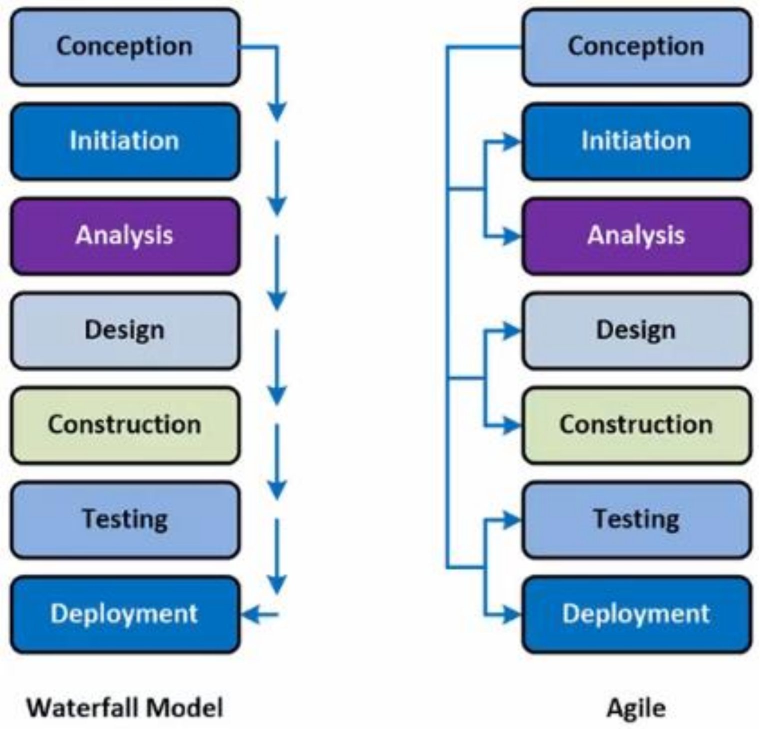
Cleanroom Model: Strictly adheres to formal steps and a more structured method. It attempts to prevent errors and mistakes though extensive testing.

Joint Analyses Development or Joint Application Development (JAD) Model: is one that uses a team approach. It uses workshops to both agree on requirements and to resolve differences.

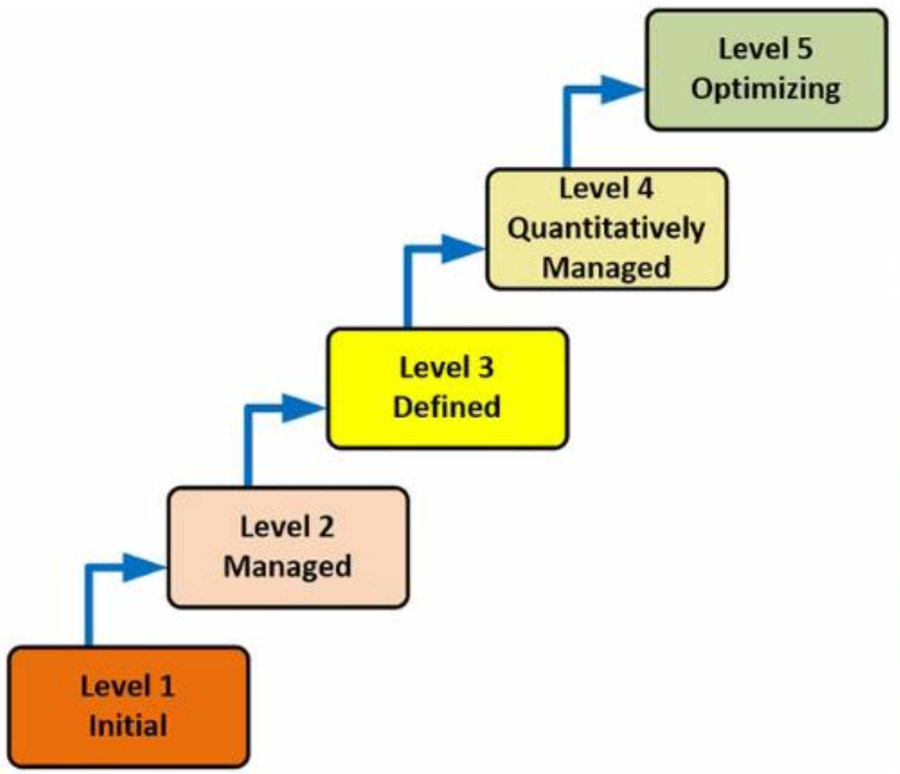
Traditional and RAD model comparison



Agile vs Waterfall:



Capability Maturity Model Integration



Programming Languages

- Machine Languages: those that deliver instructions directly to the processor
- Assembly Languages: use symbols or mnemonics to represent sections of complicated binary code
- High-Level Languages: These instructions use abstract statements like IF – THEN – ELSE and are processor independent.
- Very High Level Language: focuses on abstract algorithms that hide some of the complexity from the programmers.
- Natural Languages: The goal is to use these languages to create software that can solve problems on its own rather than require a programmer to create code to deal with a problem.

Object-Oriented Programming

- Modularity in design though autonomous objects
- Definition of internal components without impacting other parts of the system
- Reusability of components
- More readily maps to business needs

Programming Concepts

- Polymorphism: The capability of different jects with a common name to react to the same message or input with different output
- Cohesion: A term used to describe how many different tasks a module can carry out
- Coupling: Describes how much interaction one module requires form another module to do its job.
- Data Structure: Refers to the logical relationship between elements of data.

Distributed Object-Oriented System

- CORBA Common Object Request Broker Architecture is an open object-oriented standard developed by the OMG Object Management Group. This standard uses a component called the ORB Object Request Broker to implement exchanges among objects in a heterogeneous, distributed environment.
- COM Component Object Model is a model for communication between processes on the same computer.
- DCOM Distributed Component Object Model is a model for communicating between processes in different parts of the network.
- OLE Object Linking and Embedding us a method for sharing objects on a local computer that uses COM as its foundation.
- Java EE JAVA Platform Enterprise Edition is another distributed component model that relies on the Java programming language.
- SOA Service Oriented Architecture operates on the theory of providing web based communication functions without each application requiring redundant code to be written per application.
- Mobile Code: can be transferred across the network and then executed on a remote system or device.
  - Java Applet is a small component created using Java that runs in a web browser
  - ActiveX is a MS technology that uses OOP and is based on the COM and DCOM

Database Architecture and Models

- Relational Model: Uses attributes (columns) and tuples (rows) to organize data in two-dimensional tables. Each cell in the table, representing an intersection of an attribute and a tuple, represents a record.
- Hierarchical Model: Data is organized into a hierarchy. An object can have one child (an object that is a subset of the parent object), multiple children, or no children.
- Network Model: Like in the hierarchical model, data is organized into a hierarchy but unlike the hierarchical model objects can have multiple parents.

- Object-Oriented Model: Has the capability to handle a variety of data types and is more dynamic than a relational database.
- Object-Relational model: Is the marriage of Object-Oriented and Relational technologies, combining attributes of both. This is a relational database with a software interface that is written in an OOP language.

Database interface Languages

- Open Database Connectivity (DOBC) is an API that allows local or remote communication with the database
- Java Database Connectivity (JDBC) makes it possible for Java applications to communicate with the database
- XML: DB API allows XML applications to interact with more traditional databases such as relational databases
- Object Linking and Embedding Database (OLE DB) is a replacement for ODBC that extends functionality to non-relational database.

Data Warehousing and Data Mining

- Data Warehousing: the process of combining data from multiple databases or data sources in a central location called a warehouse. The warehouse is used to carry out analysis.
- Data Mining: the process of using special tools to organize the data into a format that makes it easier to make business decisions based on the content.

Database Threats

- Aggregation: The act of combining information from various sources.
- Inference: Process of piecing information together

This can become a security issue with databases when a user does not have access to a given set of data objects but does have access to them individually, or at least some of them, and can piece together the information to which they should not have access.

Access Control

- Content Dependent Access Control: access is based on the sensitivity of the data Ex. A department manager might have access to the salaries of their own employees but not to other departments employees
- Context Dependent Access Control: bases the access on multiple factors to help prevent inference. Access control can be a function of factors such as location, time of day, and previous access history.

Access Control Mechanisms

- Database Views: A given set of data a user or group can see when they access the database.
- Database Locks: Used when one user is accessing a record that prevents another user from accessing that record to prevent edit collisions.
- Polyinstantiation: A process used to prevent data interference violations by enabling a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. It prevents low-level.

Monitoring for Problems

An Online Transaction Processing (OLTP) system is used to monitor for problems such as processes that stop functioning. An ACID test endures that each transaction has the following properties before it is committed.

- Atomicity: Ether all operations are complete or the database changes are rolled back.
- Consistency: The transaction follows an integrity process that ensures data is consistent in all places where it exists.
- Isolation: The transaction does not interact with other transactions until complete.
- Durability: After it’s verified, the transaction is committed and cannot be rolled back.

Knowledge Based System

Knowledge Based System: uses artificial intelligence to emulate human logic when solving problems. They use rule-based programming to determine how to react through if-then statements and an inference engine to march patterns and facts to determine whether an operation should be allowed.

Software Threats

- Viruses
- Boot Sector virus
- Parasitic virus
- Stealth virus: constantly hides
- Polymorphic virus: constantly changes
- Macro virus
- Multipartite virus: exhibits multiple of the above

More Malware

- Worm: can spread without user assistance
- Trojan Horse: program or rogue application that is purported to do one thing but does another.
- Logic Bomb: executes based on an event
- Spyware/Adware: track internet usage to tailor ads and junk mail
- Botnet: uses network to create zombies and then attack one computer.

Rootkit

- Installs backdoors
- Removal of entries from security logs (log scrubbing)
- Replacement of default tools with compromised versions (Trojan Horse)
- Malicious kernel changes

Source Code Issues

- Buffer Overflow: Occurs when too much data is accepted as input to a specific process. It can cause an error or in some cases execute commands on the machine.
- Escalation of Privileges: Exploiting a bug or weakness in an operating system to allow a user to receive privileges to which they are not entitled.
- Backdoor: A piece of software installed by a hacker using one o the delivery mechanisms previously discussed that allows them to return later and connect to the computer without using the normal authentication process.

Malware Protection

- Antivirus software
- Antimalware software
- Security Policies

Software Security Effectiveness

- Certification is the process of evaluating the software for its security effectiveness with regard to the customer's needs. Ratings can certainly be an input to this but are not the only consideration.
- Accreditation is the formal acceptance of the adequacy of a system's overall security by the management.

Chapter 7 – Information Security Governance and Risk Management

Principles and Terms

- CIA Triad: Confidentiality ensures that data is protected from unauthorized disclosure. Integrity ensures that the data is accurate and reliable. Availability ensures that the data is accessible when needed.

- Vulnerability: An absence or weakness of a countermeasure that is in place. It can occur in software, hardware, or personnel.
- Threat: Occurs when a vulnerability is identified or exploited by an attacker.
- Threat Agents: the entity that carries out the threat. Not all agents will exploit an identified vulnerability.
- Risk: The probability that a threat agent will exploit a vulnerability and the impact if the threat is carried out.
- Exposure: Occurs when an organizational asset is exposed to losses.
- Countermeasures: A control or mechanism that reduces the potential risk. A.k.a. safeguards, controls
- Due Care: Means that an organization took all the reasonable measures to prevent security breaches and also took steps to mitigate damages causes by successful breaches.
- Due Diligence: Means that an organization investigated all vulnerabilities. This includes performing appropriate audits and assessments to ensure that the organization is protected.
- Job Rotation: Ensures that more than one person can perform job tasks, thereby providing redundancy. It is also an important tool in helping an organization to recognize when fraudulent activities have occurred.
- Separation of Duties: Ensures one person cannot compromise organizational security
  - Split Knowledge: Ensures no single employee knows all the details to complete a task
  - Dual Control: Requires that two employees must be available to complete a task.

Security Frameworks and Methodologies

ISO/IEC 27000 Series: A security program development standard on how to develop and maintain an information security management system ISMS (over 40 in all)

- 27000: Published overview of ISMS and vocabulary
- 27001: Published ISMS requirements
- 27002: Published code of practice for information security management
- 27003: Published ISMS implementation guidelines
- 27004: Published ISMS measurement guidelines
- 27005: Published information security risk management guidelines
- These standards are developed by the ISO/IEC bodies, but certification or conformity assessment is provided by third parties.
- Zachman Framework
  - An enterprise architectural framework.
  - A two-dimensional model that intersects communication interrogatives (what, where, when, why, who, and how) that intersect in a table with various viewpoints (planner, owner, designer, builder, subcontractor, actual system)
  - Allows analysis of an organization to be presented to different groups in the organization in ways that relate to the groups responsibilities.
  - Although the framework is not security oriented, using it helps you to relay information for personnel in a language and format that is most useful to them.

- The Open Group Architecture Framework (TOGAF)

  - An enterprise architectural framework
  - Helps organizations design, plan, implement, and govern an enterprise information architecture
  - Based on four inter-related domains:
    - Technology
    - Applications
    - Data
    - Business

- Department of Defense Architecture Framework (DoDAF)

  - An architectural framework
  - Organizes a set of products under four views:
    - Operational View (OV)
    - System View (SV)
    - Technical Standards View (TV)
    - All View (AV)
  - Ensures that new DoD technologies integrate properly with the current infrastructures

- British Ministry of Defense Architecture Framework (MODAF)

  - An architectural framework
  - Divides information into seven viewpoints:
    - Strategic Viewpoint (SV)
    - Operational Viewpoint (OV)
    - Service-Oriented Viewpoint (SOV)
    - Systems Viewpoint (SV)
    - Acquisition Viewpoint (AcV)
    - Technical Viewpoint (TV)
    - All Viewpoint (AV)
  - Organizations should select the enterprise architecture framework that represents the organization in the most useful manner based on the needs of the stakeholders.

- Sherwood Applied Business Security Architecture (SABSA)

  - An enterprise security framework that is risk driven
  - Like Zachman
  - Uses six communication questions (What, Where, When, Who, Why, and How) that intersect with six layers (Operational, Component, Physical, Logical, Conceptual, and Contextual).

- Control Objectives for Information and Related Technology (CobiT)

  - Security controls development framework
  - Uses a process model to subdivide IT into four deomains:
    - Plan and Organize (PO)
    - Acquire and Implement (AI)
    - Deliver and Support) (DS)
    - Monitor and Evaluate (ME)
  - Four domains are further broken down into 34 processes
  - Aligns with ITIL, PMI, ISO, and TOGAF and is mainly used in the private sector.

- National Institute of Standards and Technology (NIST)

  - Special Publication (SP) 800-53
  - A security controls development framework
  - Divides the controls into three classes
    - Technical
    - Operational
    - Management
  - Each class contains control families or categories

- SP 800-55
  - An information security metrics framework
  - Provides guidance on developing performance measuring procedures with a U.S. government viewpoint.
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework
  - A corporate governance framework
  - Consists of five inter-related components:
    - Control Environment
    - Risk Assessment
    - Control Activities
    - Information and Communication
    - Monitoring
  - CobiT was derived from the COSO framework
    - COSO is for corporate governance
    - CobiT is for IT governance

- ITIL
  - Process management development
  - Has five core publications
    - ITIL Service Strategy
    - ITIL Service Design
    - ITIL Service Transition
    - ITIL Service Operation
    - ITIL Continual Service Improvement
  - Five core publications contain 26 processes
  - Although ITIL is a security component, it is primarily concerned with managing the service level agreements (SLA's) between an IT department or organization and its customers.
  - As part of the OMB Circular A-130, an independent review of security controls should be performed every three years.

- Six Sigma
  - A process improvement standard
  - Includes two project methodologies that were inspired by Deming's Plan/Do/Check/Act cycle.
  - DMAIC includes Define, Measure, Analyze, Improve, and Control
  - DMADV includes Define, Measure, Analyze, Design, and Verify
  - Six Sigma was designed to identify and remove defects in the manufacturing process but can be applied to many business functions including security.

Security Framework and Methodologies

Capability Maturity Model Integration (CMMI)

- Process Improvement approach
- Addresses three areas of interest:
    - Product and Service development (CMMI for dev.)
    - Service Establishment and Management (CMMI for services)
    - Product Service and Acquisition (CMMI for acquisitions)
- Five levels of maturity:
    - Initial
    - Managed
    - Defined
    - Quantitatively Managed
    - Optimizing
- All processes within each level of interest are assigned on of the maturity levels

Security professionals should help their organization pick the framework that best fits the needs of the organization.

Top Down versus Bottom Up

- Top Down is initiated by Management - superior
- Bottom Up is initiated by Staff

Security Program Life Cycle

1. Plan and Organize: Risk assessment, establishing oversight and steering committee, evaluating business drivers and obtaining management approval
2. Implement: Identifying and managing assets, risks, identity and access control, training and awareness, implementing solutions, assigning roles and establishing goals
3. Operate and Maintain: Performing audits, carrying out tasks and managing the SLA
4. Monitor and Evaluate: Reviewing auditing and logs, evaluating security goals, and developing improvement plans dor integration into the Plan and Organize (Step 1)

Risk Assessment

A tool used to identify vulnerabilities and threats, assess the impact of those vulnerabilities and threats, and determine which controls to implement.

Four Main goals:

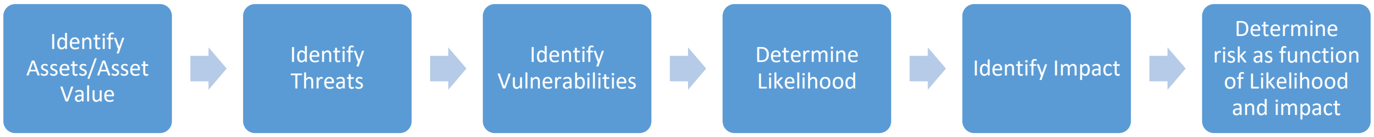
- Identify assets and asset value
- Identify vulnerabilities and threats
- Calculate threat probability and business impact
- Balance threat impact with countermeasure cost

Prior to starting the risk assessment, management and the risk assessment team must determine which assets and threats to consider, which determines the size of the project.

- The risk assessment team must provide a report to management on the value of the asset considered
- Management can then review and finalize the asset list, adding and removing as it sees fit, then determine the budget of the risk assessment project.
- If a risk assessment is not supported and directed by senior management it will not be successful.

- Management must define the risk assessment’s purpose and scope and allocate the personnel, time, and money for the project

The NIST SP 800-30 identifies the following steps in risk assessment:



Identify Assets/Asset Value → Identify Threats → Identify Vulnerabilities → Determine Likelihood → Identify Impact → Determine risk as function of Likelihood and impact

Asset Value and Threat Identification

- Tangible assets include computers, facilities, supplies, and personnel.
- Intangible assets include intellectual property, data, and organizational reputation.
- The following six considerations can be used to determine asset value:
  - Value to owner
  - Work required to develop or obtain the asset
  - Costs to maintain the asset
  - Damage that would result from losing the asset
  - Cost that competitors would pay for the asset
  - Penalties that would result if the asset was lost
- After determining the value of the asset, you should determine the vulnerabilities and threats to each asset
- Threat agents can be grouped into six categories:
  - Human: malicious and non-malicious, terrorists, spies, terminated personnel
  - Natural: Floods, earthquakes, etc.
  - Technical: hardware and software failures, malicious code and new technologies
  - Physical: CCTV issues, perimeter measures failure, and biometric failure
  - Environmental: Power and other utility failure, traffic, hazardous material spillage
  - Operational: any process or procedure that can affect CIA
- Identify vulnerabilities and threats
- Determine the loss potential for each threat by using the likelihood of the event combined with the impact that such an event would cause.
- An event with a high likelihood and a high impact would be given more importance than an event with a low likelihood and a low impact
- Different types of risk analysis, including qualitative and quantitative analysis, should be used to unsure that the obtained data is maximized

Quantitative Risk Analysis

Assigns a monetary and numeric values to all facets of the risk analysis process, including asset value, threat frequency, vulnerability severity, impact, safeguard costs, etc.

Equations are used to determine total and residual risks. The most common equations are for SLE and ALE

- Single loss expectancy (SLE) is the monetary impact of each threat occurrence.
  - To determine the SLE you need to know the Exposure Factor (EF) and the Asset Value (AV)
- Annual Loss Expectancy is the cost of the SLE times the number of times the impact is likely to occur.
- The EF is the percent value or functionality of an asset that will be lost when a threat event occurs.
- The calculation for obtaining the SLE is: **SLE = AV x EF**
  - For example, an organization has a web farm with an AV of $20k. IF the risk assessment has determined that a power failure is a threat and the exposure factor is 25% the SLE for this is $5k.

- Annual Loss Expectancy (ALE) is the expected risk factor of an annual threat event
- ALE requires SLE and the Annual Rate of Occurance (ARO) – which is how often the threat may occur annually
- **ALE = SLE x ARO**
- Using the previous example if the ARO for the power failure is 50%, then the ALE for this event is $2,500.
- These formulas are used to help an organization decide whether to implement controls.

- A purely quantitative analysis cannot be achieved because some level of subjectivity is always part of the data
- An advantage of quantitative over qualitative is that it uses less guesswork.
- Disadvantages include the difficulty of the equations, the time and effort needed to complete the analysis, and the level of data that must be gathered for the analysis.

Qualitative Risk Analysis

- Institution, experience, and best practice techniques such as brain storming, focus groups, surveys, questionnaires, meetings, interviews, and Delphi.
- Most organizations will determine the best technique(s) based on the assessed threats.
- Experience and education on threats is not needed
- Each member of the analysis group uses experience to rank the likelihoods of threat and damage
- Threat possibility, loss potential, and safeguard advantage is reported to management.
- Advantages are that the risks are prioritized and immediate improvement is recommended
- Disadvantages are the subjectivity
    - Risk Analysis always has issues with certainty. All reports include an uncertainty level listed as a percentage.

Most Risk Analysis reports include a hybrid of Quantitative and Qualitative analysis.

Most organizations favor:

- Quantitative is generally preferred to choose and substantiate costs of safeguards for tangible assets
- Qualitative for intangible assets

Safeguard Selection

- Cost effectiveness of the most common criteria for choosing
    - Planning, designing, implementing, and maintenance need to be included.
- To calculate a cost/benefit use:

(**ALE** before safeguard) - (**ALE** after safeguard) - annual cost of safeguard = **Safeguard Value**

- Implementing a safeguard can improve the ARO but will not completely do away with it.
- A legal liability exists if the cost of the safeguard is less than the estimated loss should the threat be exploited
- Maintenance is often not fully researched
    - Full researching the costs should include new staff, training, testing, etc.
- Maintenance can be hard to quantify but analysis can at least account for them.

Total Risk versus Residual Risk

- Total risk is the risk that an org can encounter if it does not implement safeguards
- Resudual risk os the remainder after safeguards are implemented
- **Residual Risk = Total Risk - Countermeasures**

    - Above equation is more conceptual than practical

Handling Risk

Risk reduction is the process of altering elements of the organization in response to risk analysis

The following four basic methods are used to handle risk:

- Risk Avoidance: Terminating the activity or choosing alternative activities
- Risk Transfer: Passing the risk to a third party, perhaps an insurance company
- Risk Mitigation: Defining the acceptable risk level and reducing the risk to that tolerance
- Risk Acceptance: Understanding and accepting the risk as well as the cost of damages

Risk Management Principles

- After the assessment is complete, the org must implement and maintain safeguards
- Continued risk analysis should be carried out on a regular basis
- Risk Management involves developing and maintaining a risk policy and a risk management team

Risk Management Policy

- Senior management must commit to the process
- The policy is a formal statement of senior management's commitment
- The policy must include the overall risk management plan and a list of risk team members as well as:
    - Risk management team's objectives
    - Roles and Responsibilities
    - Acceptable level of risk
    - Risk identification process
    - Risk safeguards mapping
    - Safeguard effectiveness
    - Monitoring process and targets
    - Future risk analysis plans and tasks

Risk Management Team

- Single team member or larger team depending on organization size
- The goal is always to protect the organization and its assets from risk in a cost-effective way
- Senior management must:
    - Specifically put a resource allocation measure in place to ensure success
    - Ensure that the team, particularly the leader, is trained and has tools
    - In a larger organization, the team leader should spend most of their time in this role.

Risk Analysis Team

- The risk analysis team must have a representative from as many areas and as many employment levels as possible
    - Having a diverse risk analysis team ensures that risks from all areas of the org can be determined
- If the team cannot contain members from all departments, the members must interview the departments
- During the process, the team should determine the threat events that could occur, the potential impact of threats, the frequency of the threats, and the level of confidence in the information gathered

Security Governance Components

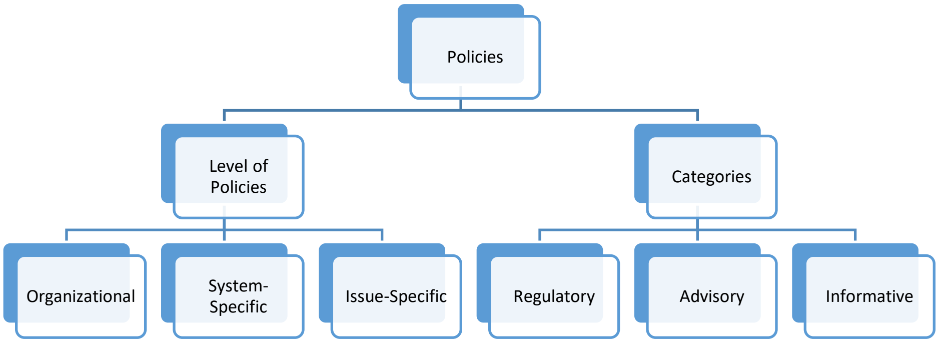
- Strategic plans guide the long-term security activities (3-5 years of more)
- Tactical plans achieve the goals of the strategic plan and are shorter in length (6-18 months)

Because management is the most critical link in the computer security chain, their approval must be obtained first when adopting an information security policy.

- Senior management must complete the following steps prior to developing an org security policy:
  - Define the scope of the security program
  - Identify all the assets that need protection
  - Determine the level of protection that each asset needs
  - Determine personnel responsibilities
  - Develop consequence for non-compliance
- By fully endorsing an organizational security policy, senior management accepts the ownership of an organizations security
- High-Level policies are statements that indicate senior managements intention to support security
- After senior management's approval is obtained, the first step is to adopt an Org Information Security Statement
- The Org Security Policy comes from this Org Information Security Statement
- The security planning process must define:
  - How security will be managed
  - Who will be responsible for setting up and monitoring compliance
  - How security measures will be tested for effectiveness
  - Who is involved in establishing the security policy
  - Where the security policy is defined
- Information security governance components include:
  - Policies
  - Standards
  - Baselines
  - Guidelines
  - Procedures
  - Information classification and lifecycle

Policies

- A security policy dictates the role of security as provided by senior management and is strategic in nature, meaning it provides the end result of security.
- Policies are defined in two ways:
  - The level in the org in which they are enforced, and
  - The category to which they are applied
- Policies are independent of a specific technology or security solution
- All policies must contain an exception area to ensure that management can deal with situations that require exceptions
- Policies are broad and provide the foundation for development the security structure which include:
  - Standards
  - Baselines
  - Guidelines
  - Procedures



- An organizational security policy is the highest level in the org and is steered by the business goals.
- An organizational security policy provides general direction and should include:
  - Define the overall goals of the security policy
  - Define the overall steps and importance of security
  - Define the security framework to meet business goals
  - State management approval of the policy, including support of security goals in principles
  - Define all relevant terms
  - Define security roles and responsibilities
  - Address all relevant laws and regulations
  - Identify major functional areas
  - Define compliance requirements and non-compliance consequences
- An organizational security policy must be supported by all stakeholders and should have high visibility and be discussed regularly
- Each version of the policy should be maintained and documented with each new release
- A system-specific security policy addresses security for a computer, network, technology, or application.
- An issue-based security policy addresses email privacy, virus checking, employee termination, no expectation of privacy, etc.
- Regulatory security policies address specific industry regulations including mandatory standards such as Healthcare, Public Utilities and Financial Institutions
- Advisory security policies provide instructions on acceptable and unacceptable activities including consequences of engaging in unacceptable activities
- Informative security policies provide information on certain topics and act as an education tool

Standards and Baselines

Standards describe how policies will be implemented within an organization and are mandatory actions and rules that are tactical in nature, meaning they provide the steps necessary to achieve security.

A baseline is a reference point that is defined and captured to be used as a future reference.

- Although capturing baselines is important, it is just as important to use them to assess the security state
- Baselines should be captured when the system is properly configured and fully updated
- New updates mean new bassline reviews and possibly new basslines

Guidelines and Procedures

- Guidelines are recommended actions that are much more flexible than standards, allowing for circumstances to occur

- Guidelines provide direction when standards do not apply
- Procures embody all the detailed actions that personnel are required to follow and are the closets to the computers and other devices
- Procures often contain step-by-step lists on how policies, standards, and guidelines are implemented

Information Classification Life Cycle

- Data should be classified based on its value to the organization and its sensitivity to disclosure
- Assigning a value to data allows the org to determine the resources to protect the data like:
    - Personnel
    - Monetary
    - Access Control
    - Etc.
- Classifying data allows you to apply different protective measures
- After data is classified, the data can be segmented based on its level of needed protection
    - The classification levels ensure that data is handled and protected in the most cost-effective manner possible
- An org should determine the classification levels it uses based on the org needs
- Several commercial business and military/government information classifications are commonly used
- The information life cycle should be based on the classification of data
- Orgs are required to retain certain information (i.e. financials) based on a local, state, or federal laws and regulations

Commercial businesses usually classify data using four levels:

- Confidential: Trade secrets, intellectual data, application programming code, etc. that can seriously affect the org if unauthorized disclosure occurred
- Private: Information related to personnel used within the org (ex. HR records, Medical, Salary)
- Sensitive: Any information that requires extra measures to ensure its CIA and accuracy
- Public: Data whose loss would not cause a negative impact on the organization

Military and Government:

- Top Secret: Includes weapons blueprints, technology specs., spy satellite information and other that can gravely damage national security
- Secret: Deployment plans, missile placement and other information that could seriously affect the government
- Sensitive but Unclassified: medical or other personnel data that would raise concerns about reputation if mismanaged
- Unclassified: Everything else and mostly falls under the public category based on the Freedom of Information Act.

All organizations need procedures in place for the retention and destruction of data

Retention and destruction must follow all laws and regulations

Documenting proper procedures ensures that information is maintained for the required time to prevent fines and incarceration of high level org officers

These procedures must include both the retention period and the destruction process.

Roles and Responsibilities

- Board of Directors: elected by shareholders

- Senior Officials: includes board of directors and senior management and must perform duties with the care that ordinary prudent people would exercise in similar circumstances (**Prudent-Man rule**)
- Management: Has the ultimate responsibility and include:
    - CEO: reports directly to the stakeholders
    - CFO: Responsible for all financials and reports to the CEO
    - CIO: Responsible for all Information and reports to the CFO or CEO
    - CPO: Responsible for privacy and reports to the CIO
    - CSO: Leads any security effort and repots to the CEO
- Business Unit Managers: Provides depart information to ensure that appropriate controls are in place for the dept.
- Audit Committee: Evaluates an org's financial reporting mechanism to ensure financial data is accurate
- Data Owner: Determines the classification level of the owned information
- Data Custodian: Implements the classification and controls
- System Owner: ensures that the appropriate controls are in place on their system(s)
    - One system has one owner, but there may be multiple data owners
- System Administrator: performs the day-to-day system operations; goal is availability
- Security Administrator: Maintains security devices and software (ex. Firewalls, antivirus, etc.); goal is security
- Security Analyst: analyzes the security needs of the org and develops the internal information and security governance documents including policies, standards, and guidelines
- Application Owner: Determines who can access the application
- Supervisor: Manages a group of users and assets owned by a group or department
- User: Any person that accesses the data to perform their job
- Auditor: Monitors user activities to ensure the proper controls are in place

Personnel Security

- Personnel are responsible for the vast majority of security issues in the org
- Organizations should have policies in place that include screening, hiring, and termination policies
- Personnel screening should occur prior to the offer of employment and may include a criminal background check, work history, credit history, driving records, substance abuse testing, and education/licensing verification.
    - Each org should determine the screening needs based on the org's needs and perspective personnel's level
- Personnel hiring procedures should include signing all appropriate documents, including government required, no expectation of privacy, and NDAs
- Employee ID's and passwords can be issued once completed
- Personnel termination must be handled differently based on whether it is friendly or un-friendly
    - Unfriendly Termination: procedures must be proactive to prevent asset damage and should include access termination and security escort from the premesis
    - Some orgs use mandatory vacations for another amployee to perform the job
- Some positions may require employment agreements to protect beyond the employment like NDAs, noncompete clauses, and code of conduct or ethics agreements.
- HR can handle org property, access, and ensuring exit interviews are completed.

Security Training

Security Awareness Training, Security Training, and Security Education are three terms that should not be interchangeable

- Security Awareness Training: reinforces the fact that valuable resources must be protected with security measures
- Security Training teaches personnel the skills needed to enable them to perform their jobs in a secure manner

- Awareness Training and Security Training are usually combined as Security Awareness Training which improves user awareness of security and ensures they can be held accountable for their actions.
- Security education is more independent and is targeted at security professionals who require security expertise to act as in-house experts for managing security programs
- Awareness training is the '*what'*, security training is the '*how'*, and security education is the '*why'*

Security Awareness Training

Security Awareness Training should be developed based on the audience

- High-Level Management: must explain potential risks and threats, effects of issues on org reputation and financial standing as well as laws and regulations
- Middle Management: policies, standards, baselines, guidelines, procedures, and how these components map to departments
- Technical Staff: configuring and maintaining controls including attack recognition. Also, this level is encouraged to pursue education and certifications.
- Regular Staff: need to understand their responsibilities regarding security so that they perform their day-to-day tasks securely. Providing real world examples is effective with this group
- Personnel should sign a document that indicates they have completed training and understand all the topics
- Although initial training should occur when on-boarding, security awareness should be a continuous process, with future training occurring at least annually.

Security Budget, Metrics, and Effectiveness

- The CSO or other designated high-level manager prepares the org's security budget, determines the metrics, and reports on the effectiveness of the program.
- The budgeting process requires an examination of all risks and ensures that security projects with the best cost-benefit ratio are implemented. Security metrics provide information on both short and long term trends.
    - By collecting these metrics and comparing them on a day-to-day basis, a security professional can determine the daily workload
    - Procedures should state who will collect the metrics, which metrics will be collected, when the metrics will be collected, and what thresholds will trigger the corrective actions
    - The security metrics should be analyzed by a third party and analytical data from a third party should be used to improve the security program and security metrics process

Chapter 8 Telecommunications and Network Security

OSI Model: Breaks up the communication process into layers with standardized interfaces between layers, allowing for single layer changes. It provides a common framework for hardware and software developers, fostering interoperability.

Application Layer

Receives raw data from the application in use and provides services such as file transfer and transfer message

Examples:

- HTTP
- DNS
- FTP
- SMTP

Presentation Layer

Responsible because the data from the application layer is represented (or presented

Examples:

- MIME
- XDR

Session Layer

Responsible for adding information to the packet that makes a communication session between a service or application on the source device possible with the same service or application on the destination device.

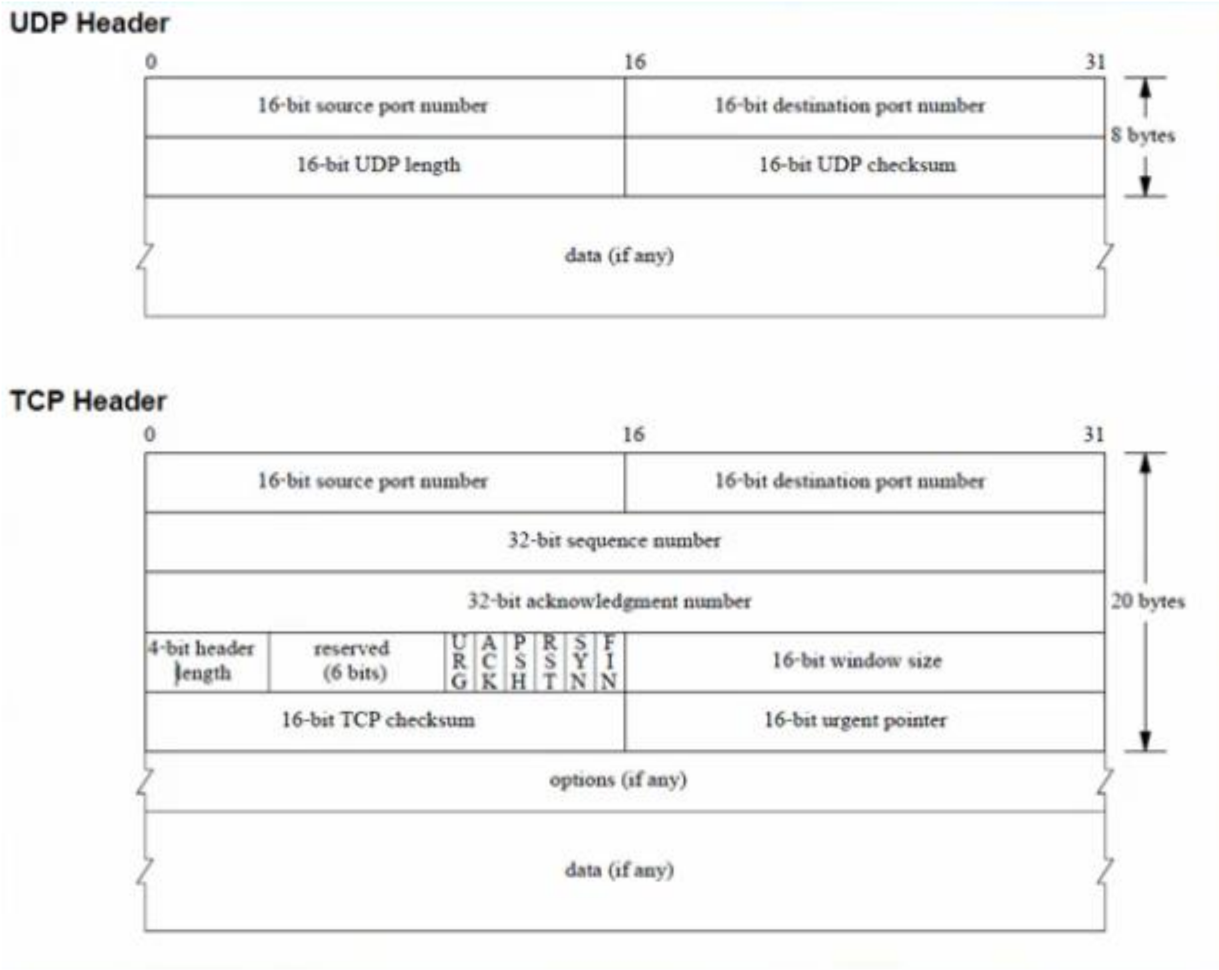
The application or service in use is communicated between the two systems with an identifier called a port number.

Transport Layer

Establishes a session between the two physical systems which can be connection-oriented or connectionless.

- TCP
- UDP

At this layer, the PDU is called a segment.



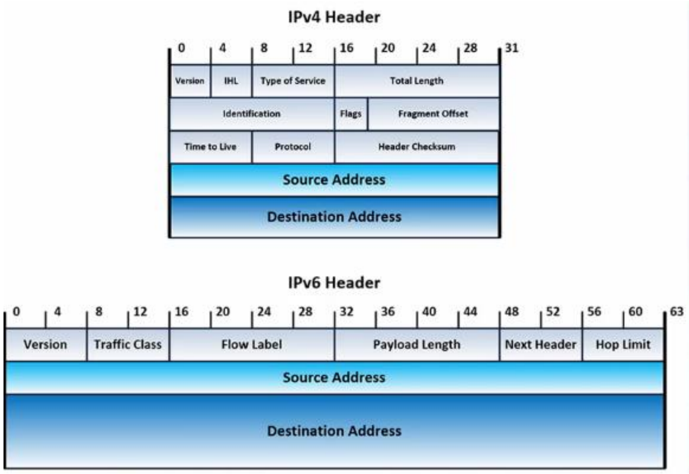
Three-way handshake for TCP/IP

- SYN →
- SYN/ACK ←
- ACK →

Network Layer

- Information required to route the packet is added in the form of a source and desitnation logical address.
- In TCP/IP, this is in terms of a source and destination IP address
- At this layer, the PDU is called a packet
- Examples:
    - IP Internet Protocol
    - ICMP Internet Control Message Protocol
    - IGMP Internet Group Management Protocol
    - ARP Address Resolution Protocol

IPv4 vs. IPv6



Data Link Layer

- Responsible for determining the destination physical address
- In ethernet this is called the Media Access Control (MAC) address
- Also, added a trailer at the 'end' of the frame to confirm integrity
- At this layer, the PDU is called a frame

Physical Layer

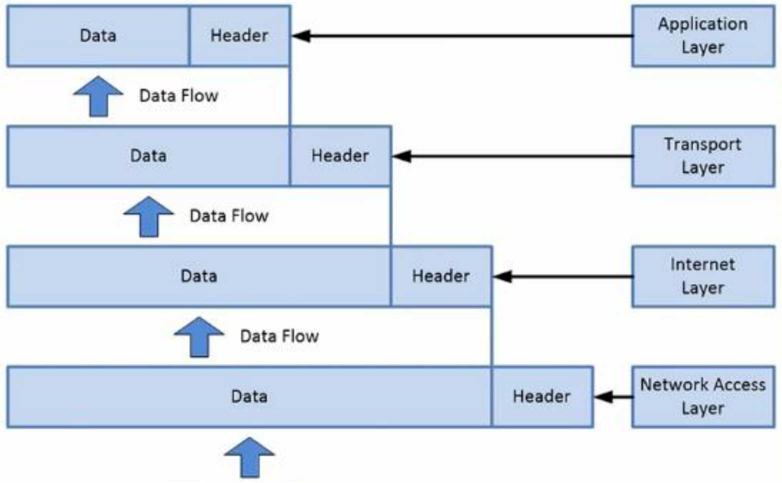
- Responsible for turning all the information into 1's and 0's and sending it out
- Accomplished by different methods according to media

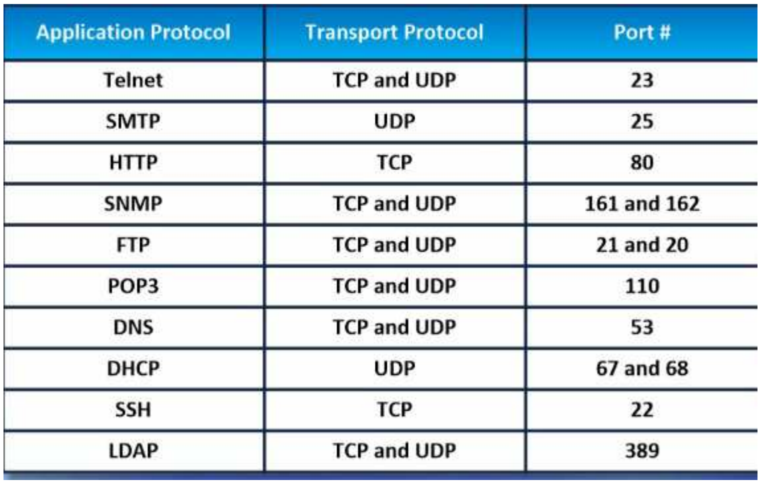
TCP/IP Model

Four Layers

TCP/IP	**OSI**
Application	Application
	Presentation
	Session
Transport	Transport
Network	Internet
Network Access	Data-Link
	Physical

Encapsulation





Application Protocol	Transport Protocol	Port #
Telnet	TCP and UDP	23
SMTP	UDP	25
HTTP	TCP	80
SNMP	TCP and UDP	161 and 162
FTP	TCP and UDP	21 and 20
POP3	TCP and UDP	110
DNS	TCP and UDP	53
DHCP	UDP	67 and 68
SSH	TCP	22
LDAP	TCP and UDP	389

IP Addressing

External:

- Class A: 0.0.0.0 – 127.255.255.255
- Class B: 128.0.0.0 – 191.255.255.255
- Class C: 192.0.0.0 – 223.255.255.255

Internal:

- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255

IP4 vs. IP6

192.168.5.5 4 is 32-bit in octets

2001:00000:4137:9e76:30ab:3035:b541:9693 is 128-bit in hexadecimal sextets

MAC Addressing

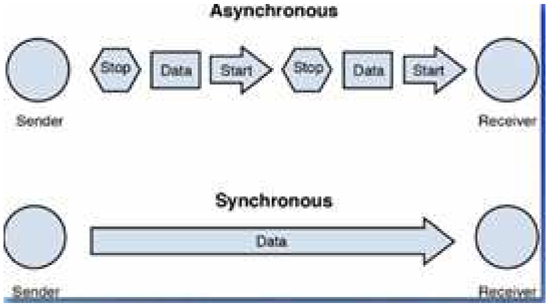
48-bit addresses in hex on the NIC

01:23:34:67:89:ab

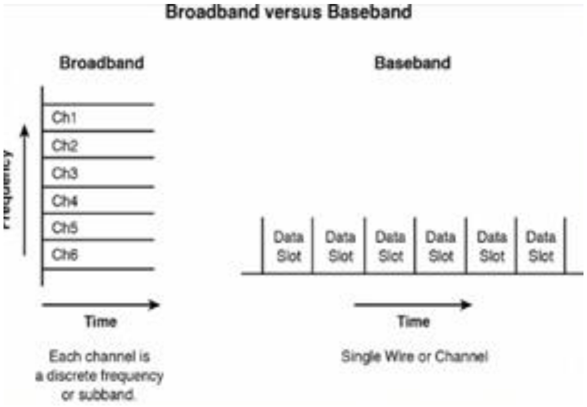
At every router hop it changes

Analog wave vs. Digital transmission

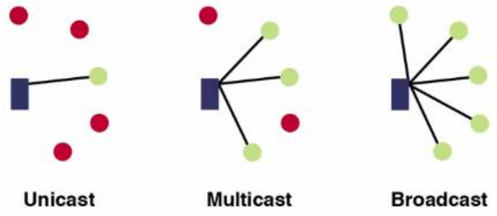
Asynchronous vs. Synchronous



Broadband vs. Baseband



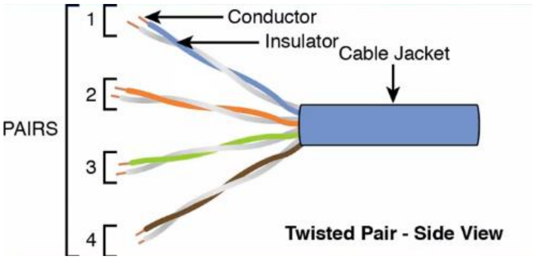
Unicast, Multicast, and Broadcast



Wired vs. Wireless

- 802.2 Wired Ethernet
- 802.11 WLan
- 802.16 WiMax

Twisted Pair

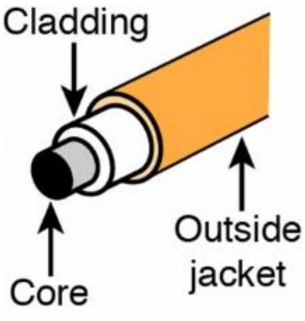


Twisted Pair Variants

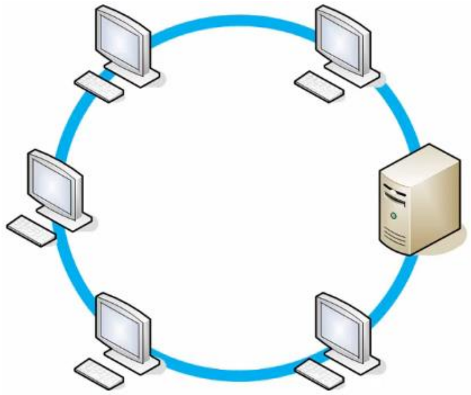
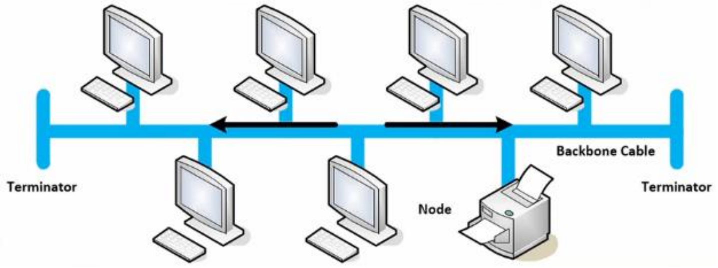
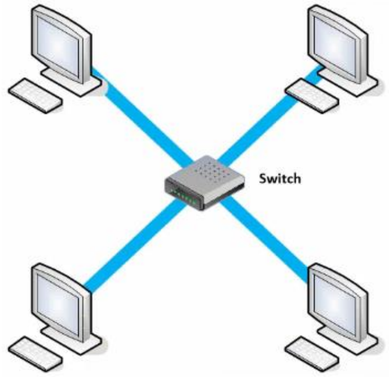
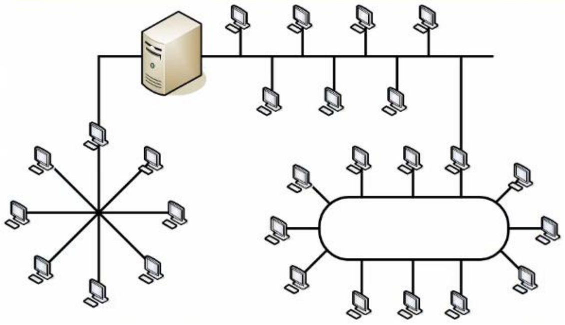
- 10BaseT: Operates at 10 Mbps
- 100BaseT: Operates at 100 Mbps (Fast Ethernet)
- 1000BaseT: Operates at 1000 Mbps (Gigabit)
- 10GBaseT: Operates at 10 Gbps

Name	Maximum Speed
Cat3	10 Mbps
Cat4	16 Mbps
Cat5	100 Mbps
Cat5e	100 Mbps
Cat6	1 Gbps
Cat6a	10 Gbps

Fiber Optic



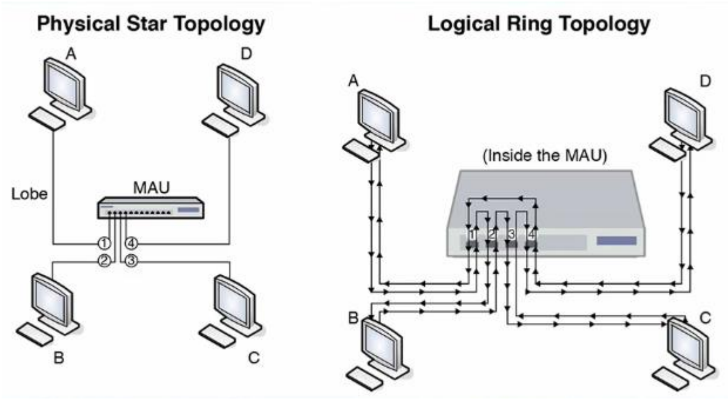
Network Topologies

Ring 	Bus 
Star  	Hybrid 

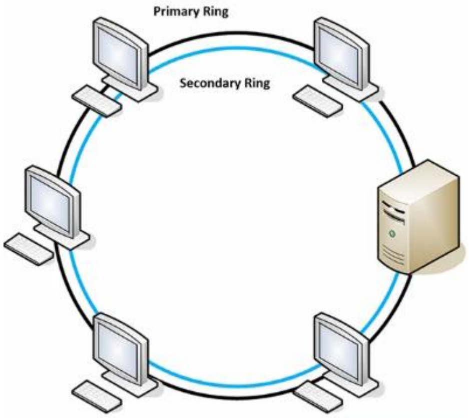
Ethernet

Ethernet II							
Preamble 8 bytes	DA 6 bytes	SA 6 bytes	Type 2 bytes	Data	FCS 4 bytes		
802.3 Ethernet							
Preamble 8 bytes	DA 1 bytes	DA 6 bytes	SA 6 bytes	Length 2 bytes	802.2 Header	Data	FCS

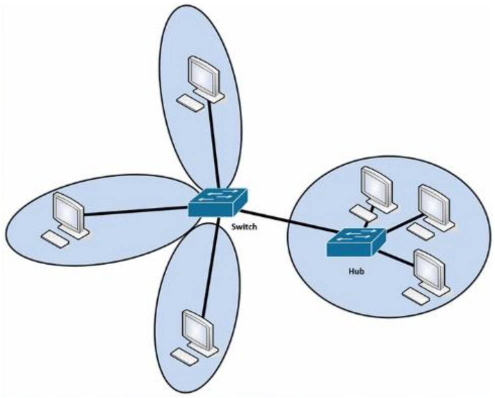
Token Ring 802.5



Fiber Distributed Data Interface (FDDI)



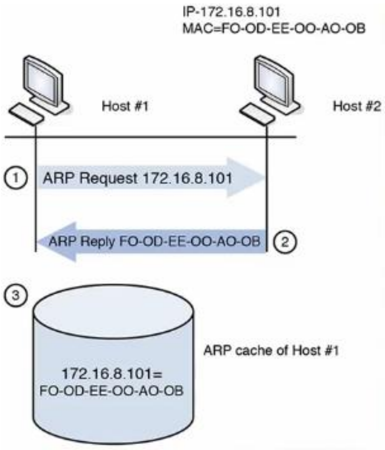
Collision Domains



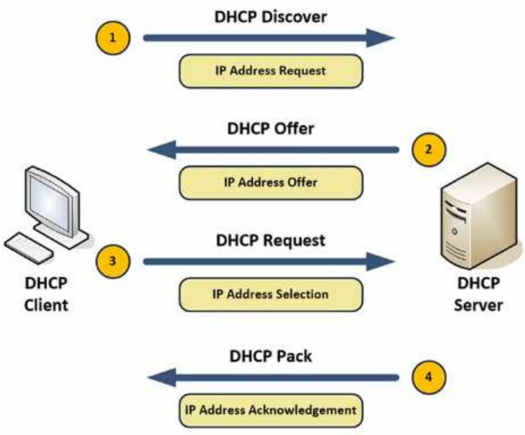
Contention Methods

- CSMA/CD
- CSMA/CA
- Token Passing
- Polling

ARP



DHCP



Other Network Protocols and Services

- DNS
- FTP, FTPS, SFTP
- HTTP, HTTPS, SHTTP
- ICMP
- IMAP
- NAT
- POP
- SMTP
- SNMP

Network Routing

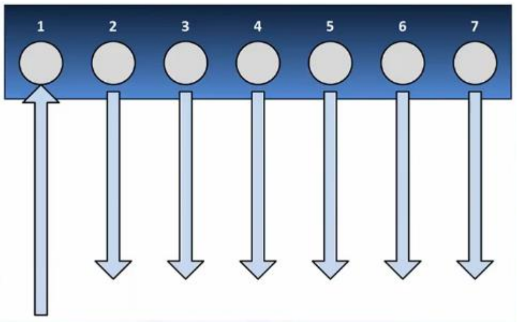
- Routing occurs at Layer 3 of the OSI model.
- Routing protocols can be either distance vector or link state
- Standard protocols include RIP, IS-IS, OSPF, BGP, and VRRP

- Proprietary protocols include IGRP and EIGRP

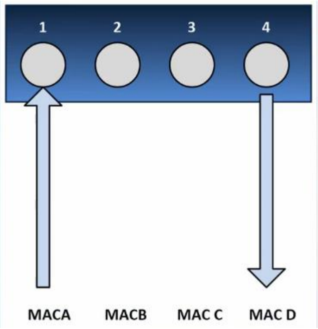
Network Devices

- Patch Panels: Operates at OSI 1 and functions as a central termination point for all cables
- Multiplexor: Operates at OSI 1 and functions to combine several input information signals to one output signal

Hub



Switch



Other Devices

- Routers: uses a routing table that tells the router in which direction to send traffic destined for a particular network
- Gateway: any device that performs some sort of translation or acts as a control point to enter and exit

Firewall Architectures

- Bastion Host
- Dual-Homed
- Three-Legged
- Screened Subnet

Other Devices

- Proxy Server
- PBX
- Honey Pot

Cloud Computing

- IaaS: Infrastructure as a Service is when the vendor provides hardware
- PaaS: Infrastructure as a Service is when the vendor provides hardware and the software on the hardware

- SaaS: Software as a Service is when the vendor provides turnkey

Network Types

- LAN
- Intranet
- Extranet
- MAN
- WAN

WAN Technologies

- T Carriers

Carrier	T1's	Channels	Speed Mbps
Fractional	1/24	1	.064
T1	1	24	1.544
T3	28	672	44.736

- E Carriers

Signal	Rate
E0	64 Kbps
E1	2.048
E3	8.448

OC Lines SONET

Optical Carrier	Speed
OC-9	466.5 Mbps
OC-19	933.12 Mbps
OC-48	2.488 Gbps
OC-3072	160 Gbps

CSU/DSU

Channel Service Unit/Data Service Unit connects a LAN to a WA. This is considered a Data Communication Device Equipment (CDE) device and provides an interface for the router which is a Data Terminal Equipment (DTE) device.

Circuit Switching vs. Packet Switching

- Circuit switches (like telephones) establish a set path to the destination
- Packet switching uses packet based paths

Additional WAN Technologies

- Frame Relay
- ATM
- X.25
- Switched Multimegabit Data Service
- Point-to-Point Protocol
- High Speed Serial Interface
- PSTN (POTS, PBX)

VOIP security

- Separate VLan to prevent VOIP access from PC's
- VOIP aware firewalls
- Ensure all VOIP passwords are strong
- Secure the network layer with IPsec

Remote Connection Technologies

- Dial-Up
- ISDN
- Cable
- DSL

Dial-Up

ISDN

- BRI: Basic Rate provides three channels (144 Kbps)
  - 2 B channels 64kbps each
  - 1 D channel 16 Kbps
- PRI: Primary Rate (1.54 Mbps)
  - 23 B channels
  - 1 D channel

Cable

DSL

- SDSL: Symmetric usually provides from 192 Kbps to 1.1 Gbps
- ADSL: Asynchronous usually provides uploads from 192 – 384 Kbps and 768 Kbps down
- HDSL: provides T-1 speeds
- VDSL: provides service for HDTV and VOIP

VPN Components

LAN Protocol (TCP/IP)

1. Remote Protocol
   - PPTP: point to point tunneling
   - L2PT Layer 2 Tunneling Protocol
2. Authentication Protocol (optional)
   - CHAP
   - MS-CHAP
   - EAP-TLS
3. Encryption Protocol (optional)
   - MPPE
   - IPsec

IPsec Components

- AH: Authentication Header provides data integrity, data origin authentication, and protection from replay attacks
- ESP: Encapsulation Security Payload provides all that AH does and well as data confidentiality.
- ISAKMP: Internet Security Association and Key Management Protocol handles the creation of a security association for the session and the exchange of keys.

- IKE: Internet Key Exchange (a.k.a. IPsec Key Exchange) provides the authentication material used to create the keys exchanged by ISAKMP during peer authentication.

RADIUS and TACACS

Networking protocols that provide centralized authentication and authorization for:

- Dial-Up remote access servers
- VPN access servers
- Wireless Access Points
- Security-enabled switches

Remote Authentication Protocols

- PAP: Password Authentication Protocol
- CHAP: Challenge Handshake Authentication Protocol
- EAP: Extensible Authentication Protocol

TLS/SSL Transport Layer Security/Secure Socket Layer

- SSL Portal VPN: in which a user has a single SSL connection used to access multiple services on the web server. After being authenticated, the user is provided a page that acts as a portal to other services.
- SSL Tunnel VPN: uses an SSL tunnel to access services on a server that is not a web server. It uses custom programming to provide access to non-web services through a web browser.

Wireless Networks 802.11 Techniques

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DHSS)
- Orthogonal Frequency Division Multiplexing (OFDM)

Wireless Networks Cellular or Mobile Wireless Techniques

- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)
- Orthogonal Frequency Division Multiple Access (OFDMA)
- Global System Mobile (GSM)

WLAN 802.11 Standards

802.11a	2.4 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	5.0 GHz	54 Mbps
802.11n	Both	650 Mbps
802.11ac	5.0 GHz	6 Gbps

Wireless Networks Short Range

Bluetooth: used to create personal area networks (PANs). These are simply short-range connections that are between devices and peripherals such as headphones. It operates in the 2.4 GHz frequency at speeds of 1-3 Mbps at a distance up to 10 meters

Infrared: Used for short connections between devices that both have an infrared port. It operates up to 5 meters at speeds of 4Mbps

WLAN Security Models

- WEP
- WPA
- WPA2
- Hidden SSID
- MAC Filter

WPA and WPA2

Variant	Access Control	Encryption	Integrity
WPA Personal	Pre-Shared key	TKIP	Michael
WPA Enterprise	802.1x (RADIUS)	TKIP	Michael
WPA2 Personal	Pre-Shared key	CCMP, AES	CCMP
WPA2 Enterprise	802.1x (RADIUS)	CCMP, AES	CCMP

Network Cable Threats

- Noise
- Attenuation
- Crosstalk
- Eavesdropping

ICMP Attacks

- Ping of Deatj
- Smurf
- Fraggle
- ICMP Redirection
- Ping Scanning

DNS Attack

- DNS Cache Poisoning
- DoS
- URL Hiding
- Domain Grabbing
- Cybersquatting

Email Attacks

- Email Spoofing
- Spear Phishing
- Whaling
- Spam

Wireless Attacks

- Wardriving: the process of riding around with a wireless device connected to a high-power antenna searching for WLANs. It could be for obtaining free Internet access or it could be to identify any open networks vulnerable to attack.

- Warchalking: A practice that typically accompanies wardriving. When a driver locates a WAN they document the SSID, traditionally in chalk in public places, but mostly online today.

Other Attacks

- SYN ACK attacks
- Session Hijacking
- Port Scanning
- Teardrop
- IP Address Spoofing

Chapter 9 - Operations Security

Concepts

- Need-to-Know/Least Privilege: Give users access only to resources required to do their job.
- Separation of Duties: Ensures that no single individual can compromise a system.
- Job Rotation: Enhances the opportunity to discover unusual activity.
- Sensitive Information Procedures: Protect against the private information of customers and employees.
- Record Retention: Retain and review all auditing records.
- Monitor Special Privileges: Rights carry with them a responsibility to exercise the rights responsibly and ethically.

Protecting Tangible and Intangible Assets

Facilities

- Do doors close automatically, and does an alarm system sound if they are opened too long?
- Are the protection mechanisms of sensitive areas, such as server rooms, sufficient and operational?
- Does the fire suppression system work?
- Are sensitive documents shredded as opposed to being thrown in the dumpster?

Hardware

- Change all default administrator passwords on devices.
- Limit the number of users that have remote access to devices.
- Rather than Telnet use encrypted command line tools like SSH.
- Manage critical systems locally.
- Limit physical access to devices.

Software

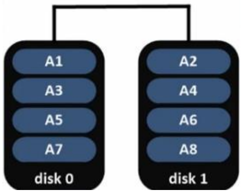
- Monitor the use of commercial applications to prevent unintentional breach of licensing
- Information assets: Recipes, processes, trade secrets, product plans, and any other type of information that enables the enterprise to maintain competitiveness.
-

Asset Management

(Ensuring Availability, Authorization and Integrity)

- Redundancy and Fault Tolerance: Enhances availability
- Backup and Recovery Systems: Facilitates quick recoveries
- Identity and Access Management: Supports integrity of information

Media Management

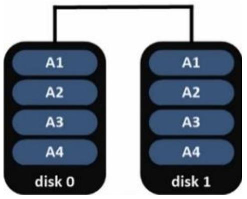
Raid 0 • Raid 0 is disk striping and writes data across multiple drives • Although it improves performance it does not provide fault tolerance	 A1 A3 A5 A7 disk 0 A2 A4 A6 A8 disk 1

<table>
<tr>
<td>

Raid 1

- Mirroring by using 2 disks and writes a copy of the data to both disks
- Provides fault tolerance

</td>
<td>

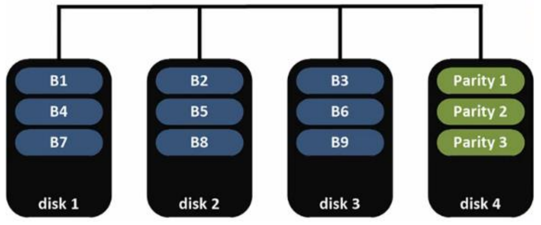


</td>
</tr>
<tr>
<td>

Raid 3

- Requires at least 3 drives
- Data is written across all drives like striping and
- Parity information is written to a single dedicated drive

</td>
<td>

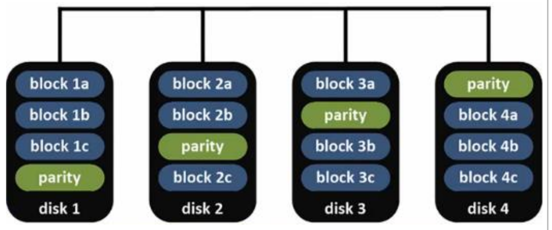


</td>
</tr>
<tr>
<td>

Raid 5

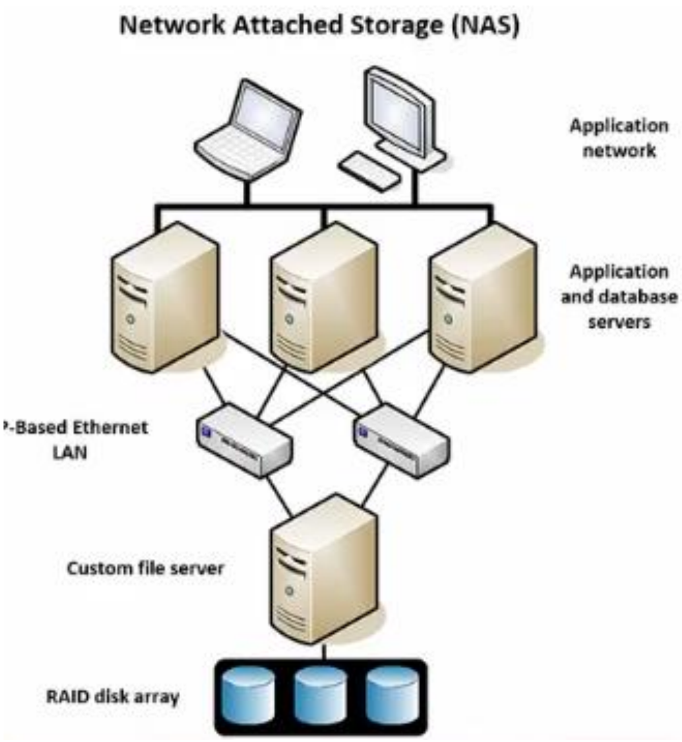
- Requires at least 3 drives
- Data is written across all drives like striping
- Parity information is written across all drives removing a single point of failure

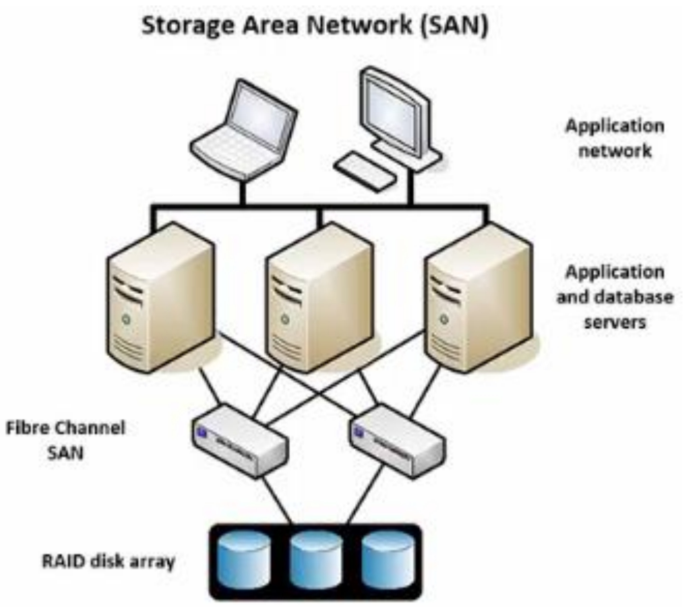
</td>
<td>



</td>
</tr>
</table>

Storage Options





Storage Management Issues

- Hierarchical Storage Management (HSM): A type of backup management that provides a continuous online backup using optical storage or tape jukeboxes. It operates automatically moving data between high-cost and low-cost media as the data ages.
- Media History: Accurately maintain a media library logs to keep track of the history
- Media Labeling and Storage: Plainly label all forms of storage media (tapes, optical, etc.) and store them safely.
- Environment: Magnetic media damage occurs above 100 degrees.

Sanitizing and Disposing of Data

- Data Purging: Using a method such as degaussing to make the old data unavailable even when using forensics.
- Data Clearing: Renders information to be unrecoverable from a keyboard.
- Remanence: Any data left after the media has been erased.

Network and Resource Management

- Redundant hardware: Speeds recoveries from hardware failure.
- Fault-tolerant technologies: Enhances availability.
- Service Level Agreements (SLA's): Introduce predictability to problem responses.
- MTBF and MTTR: Enhance the planning process.
- Single Point of Failure (SPOF): should be identified and eliminated.

Incident Response Management Steps

1. Detect
2. Respond
3. Report
4. Recover
5. Remediate
6. Review

Change Management

- All changes should be formally requested
- Each request should be analyzed to ensure it supports all goals and policies
- Prior to formal approval, all costs and effects of the methods should be reviewed
- After approval, the change steps should be developed
- During implementation, incremental testing should occur, relying on a predetermined fallback strategy if necessary
- Complete documentation should be produced and submitted with a formal report to management

Audit and Review

When assessing controls over audit tails or logs one should address the following:

- Does the trail provide a trace of user actions?
- Is access to the online logs strictly controlled?
- Is there a separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Threats and Preventative Measures

- Clipping levels: set a baseline for normal user errors, and violation exceeding that threshold are recorded for analysis.
- Deviations from Standards: help identify certain types of DoS attacks
- Unusual or unexplained events: root causes of issues must be identified
- Unscheduled reboots: typically, a sign of hardware problems
- Input/Output Controls: apply controls or checks to the input that is allowed and the be submitted to the system

Trusted Recovery: when an application or operating system suffers a failure it is important that the system respond in a way that leaves the system in a secure state.

Trusted Paths: a communication channel between the user or the program and the **trusted computer base**. **TCB** provides the resource s to protect the channel and prevent it from being compromised.

System Hardening

- Remove unnecessary applications
- Disable unnecessary services
- Block unrequired ports
- Tightly control the connecting of external storage devices and media (if allowed at all)

Monitoring and Reporting

- Vulnerability Management System: Software that centralizes and can automate the process of continual monitoring for network vulnerabilities
- IDP/IPS: Must be updated on a regular basis with the attack signatures that enable them to detect new attack types.
- Reduce the collected data when monitoring as much as possible whilst satisfying requirements.
- Ensure that report formats reflect the technical level and needs of the audience.

Chapter 10 – Business Continuity and Disaster Recovery

Concepts

Disruption: Any unplanned event that results in the temporary interruption of any organization asset, including processes, functions, and devices.

Three disruption categories:

- Nondisasters: temporary interruption due to malfunction or failure. May or may not require public notification.
- Disaster: a suddenly occurring event that has a long-term negative impact on life.
    - An emergency that goes beyond the normal response of resources
    - Usually affects a wide geographic area and results in severe damage, injury, loss of life and property.
    - Severity of financial and reputation damage depends on the time the org takes to recover
    - A disaster is officially over when all business elements have returned to normal at the original site
    - Primary concern is always personnel safety
- Catastrophe: a disaster that has a much wider and much longer impact like when a building is destroyed.

Causes of disasters are categorized by their origin:

- Technological: when a device fails.
    - It can be from:
        - device defects
        - incorrect implementation
        - incorrect monitoring
        - human error
    - Not typically international
    - If the failure is the result of a deliberate attack then it is classified as man-made
    - Historically, all tech failures were considered man-made, now they are separated but often related.
- Man-Made: occur through human intent or error.
    - Examples:
        - Enemy attacks
        - Bombings
        - Sabotage
        - Arson
        - Terrorism
        - Anything that creates a personnel unavailability due to emergency evacuation
    - In most cases, man-made are intentional
- Natural: occur because of a natural hazard.
    - Examples:
        - Flood
        - Tsunami
        - Hurricane
        - Earthquake
        - Tornado
        - Fire (that is not the result of arson)

Disaster Recovery minimizes the effect of a disaster and includes the steps necessary to resume normal operation.

- Disaster Recovery must take into consideration all org resources, functions, and personnel
- Each org function or system will have its own Disaster Recovery Plan (**DRP**)
- The DRP is created as a direct result of being identified in the Business Continuity Plan (**BCP**)
- The DRP is implemented when the emergency occurs and includes steps to prevent loss of life, prevent loss or damage to property, and restore the system

Continuity Planning deals with identifying the impact of any disaster and ensuring that a viable recovery plan for everything is implemented

- The primary focus is how to carry out org functions when a disruption occurs
- The BPC considers all aspects that are affected by a disaster including:
    - Functions
    - Systems
    - Personnel
    - Facilities
- The BPC lists and prioritizes the services that are needed, particularly the telecommunications and IT functions
- A Business Impact Analysis (BIA) is a functional analysis that occurs as part of business continuity and D.R.
    - Performing a thorough BIA will help business units understand the impact of a disaster
    - The resulting document produced from a BIA lists the critical and necessary functions, their resource dependencies, and their level of criticality to the overall organization.

BCP Concepts

- Although the BCP defines the organizational aspects that can be affected and the DRP defines how to recover functions and systems, the contingency plan provides instruction on what personnel should do until the functions and systems are resorted to full function
    - It usually contains contact information for all personnel, vendor contract information, and equipment and system requirements.
- Failure of the contingency plan is usually considered a management failure
- A contingency plan, along with BCP and DRP, should be reviewed annually
- As with all such plans, version control should be maintained
- Copied should be provided to personnel for storage both onsite and offsite to ensure that personnel can access the plan in the event of the destruction of the organization’s main facility
- Availability is a main component of business continuity planning
- The org must determine the acceptable level of availability for each function or system
- If the availability of a resource falls below this defined level, then specific action must be followed to ensure that availability is restored
- Reliability is the capability of a function or system to consistently perform according to specification
- It is vital in business continuity to ensure that the org’s processes can continue to operate. Reliability replaces emphasis on process
- Recoverability is the capability of a function or system to be recovered in the event of a disruption.
- As part of recoverability, downtime must be minimized.
- Fault Tolerance is provided when a backup component begins operation when the primary component fails.
- Varying levels of fault tolerance can be achieved based on how much an org is willing to spend, The backup components tend to not provide the same level of service as the primary component.

BIA Development

- The BCP development depends most on the development of the BIA
- The BIA helps the org to understand what impact a disruptive event would have on the org
- The four main steps of the BIA follow:
    1. Identify critical processes and resources
    2. Identify outage impacts and estiamte downtime
    3. Identify resource requirements
    4. Identify revcovery priorities
- The BIA relies heavily on any vulnerability analysis and risk assessment that is completed
- The vulnerbility analysis and risk assessment may be perfoemed by the BCP committee or by a seperately appointed risk assessment team.

Identify Critical Processes and Resources

- When identifying the critical processes and resources of an org, the BCP committee must first identify the org's business units or functional areas
- After all units have been identified the BCP team should select which individuals will gather all the needed data and select how to obtain the data
- These individuals will gather the data using a variety of techniques, including questionairres, interviews, and surveys
    - There may also be a vulnerability analysis and risk assessment or use the results of these tests as input for the BIA
- The org's buseinss proceesses and functions and the resources upon which they depend should be documented
    - This list should include all buseinss assets, including physical and financial assets that are owned by the org, and any assets that provide competetive advantages or credibility

Identify Outage impacts

- Identify outage impacts and estimate downtime
- After determining all the business processes, functions, and resources the org should then determine the criticalities.
- As part of this, you need to understand the following terms:
    - Maximum Tolerable Downtime (MTD) or Maximum Period Time of Disruption (MPTD): tolerance for a system
    - Mean Time to Repair (MTTR): The average time required to repair a single resource or function
    - Mean Time Between Failures (MTBF): The amount of time a device will operate before a failure
        - Provided by vendor
        - System reliability is increased by a higher MTBF and a lower MTTR
    - Recovery Time Objective (RTO): The shortest time after a disaster within which a resource must be restored to avoid unacceptable consequences. The RTO should be smaller than the MTD
    - Work Recovery Time (WRT): The difference between RTO and MTD, which is the remaining time after the RTO but before the reaching the MTD
    - Recovery Point Objective (RPO): The point in time to which the disrupted resource must be returned

Identify outage impacts and estimate downtime

- Each org must develop its own documented criticality levels, like the following examples:
    - Critical: resources are most vital and should be restored within minutes or hours
    - Urgent: resources should be restored within 24 hours
    - Important: should be restored within 72 hours
    - Normal: resources should be restored within 7 days

Identify Resource Requirements

- Resource requirements should also consider any human resource requirements
- When human resources are unavailable the org can be just as negatively impacted as when tech resources are not available
- The org must document the resource requirements for every resource that would need to be restored when the disruptive event occurs
    - This includes device name, OS or platform version, hardware requirements, and interrelationships

Identify Recovery Proorities

- After all the resource requirements have been identified, the org must identify the recovery priorities
- Establish recovery priorities by taking into consideration:
    - Process criticality
    - Outage impacts
    - Tolerable downtime
    - System resources
- After all this information is compiled the result is an information system recovery priority hierarchy
- Three main levels of recovery priority should be used: High, Medium, and Low
- The BIA stipulates the recovery priorities but does not provide the recovery solutions; those are in the DRP

Business Continuity Scope and Plan

- The most important personnel in the development of the BCP is senior management
    - Senior management support of BCP and DRP drives the overall organizational view of the process
- Senior management sets the overall goals of BC and DR
- A BC coordinator should be named by senior management and leads the BCP committee
- The committee develops, implements, and test the BCP and DRP
    - The committee should contain a member from each business unit
    - At least one member of senior management should be part of the committee
- The org should ensure that IT, Legal, Security, and Communications are represented
- With management direction, the BCP committee must work with the business to determine the continuity and disaster recovery priorities
- Senior business unit managers are responsible for identifying and prioritizing time-critical systems
- After all the plan is complete, the BCP committee should review it regularly to ensure it remains current and viable
- A BC project without a limited scope can often become too large for the committee to handle correctly
- For this reason, senior management might need to split the project into smaller, more manageable pieces
- When considering the splitting of the BCP, and org may want to split by geographic location or facility
- Eventually, an enterprise wide BCP should be developed that ensures compatibility with the individual plans
- One of the most popular business continuity and disaster recovery planning standards is Special Publication 800-35 Revision 1 (SP 800-35-R1) from the National Institute of Standards and Technology (NIST).

Preventive Controls

- Identifying preventative controls is the third step of the business continuity steps per NIST SP 800-34 R1
- Preventative methods are preferable to actions that might be necessary to recover the systems after a disruption if the methods are feasible and cost effective

- In anticipation of disasters and disruptive events, orgs should implement redundancy for critical systems, facilities, and power and assess whether implementation of redundancy is cost effective.
- Redundancy occurs when an org has a secondary component, system, or device that takes over during failure
- Redundant facilities ensure that the organization maintains a facility at whatever level it chooses to ensure that the services can continue when a disruptive event occurs
- Power redundancy is implemented using Uninterruptable Power Supplies (UPS's) and power generators
- Fault tolerance enables a system to continue operation in the event of a failure of one or more components
- Fault tolerance within a system can include fault tolerant adapter cards and fault tolerant storage drives
- By implementing fault tolerance tech, an org can ensure that normal operation occurs if a single component fails
- Although redundancy and fault tolerance can actually act as a preventative measure, insurance is not technically a preventative measure.
- If the org purchases insurance to provide protection in the event of a disruption, the insurance has no power to protect against the event itself. The purpose of the insurance is to ensure that the organization will have access to additional financial resources to help in the recovery.
- By purchasing insurance, the org can ensure that key financial transactions, including payroll, accounts payable, and any recovery costs are covered.
- Insurance actual cost valuation (ACV) compensates property based on the value of the item on the date of loss plus 10%.
- A special type of insurance called business interruption insurance provides monetary protection for expenses and lost earnings.
- Organizations should annually review insurance policies and update them as necessary
- Data backup provides prevention against data loss but not prevention against the disruptive event
- All orgs should ensure that all systems that store important files are backed up in a timely manner
  - Users should also be encouraged to back up personal files that they might need
- Periodic testing of the restoration process should occur to ensure that the files can be restored
- Orgs should implement fire detection and suppression systems as part of any BCP

Create Recovery Strategies

- Higher level recovery strategies identify the order in which processes and functions are restored
- System level recovery strategies define how a system should be restored
  - Keep in mind those individuals who best understand the system should define the system recovery strategies
- Although the BCO committee can develop the prioritized recovery lists and high level recovery strategies, system administrators and other IT personnel need to be involved in the strategies for IT assets
- Disaster recovery tasks include recovery procedures, personnel safety procedures, and restoration procedures.
- The recovery plan committee receives its direction from the BCP and senior management
- All decisions regarding recovery should be made in advance and incorporated into the DRP
- As part of the DRP, the recovery plan committee should contact critical vendors ahead of time to endure that any equipment or supplies can be replaced in a timely manner
- When a disaster occurs, the orgs spokesperson should report the bad news in an emergency press conference before the press learns of the news through another channel
  - The DPR should detail any guidelines for handling the press.
  - The emergency press conference site should be planned
- When resuming normal operations after the event, the org should conduct a thorough investigation if the cause of the event is unknown

- Personnel should account for all damage related costs that occur because of the event
- Appropriate steps should be taken to prevent further damage to property
- The commonality between all recovery plans is that they all become obsolete. They require testing and updating.

Categorize Asset Priority

- The recovery plan committee must understand the backup and restore solutions that are available and implement the system that will provide recovery within the BIA values in cost constraints.
- The window of time for recovery of data processing capabilities is based on the criticality of the operations affected.
- The recovery plan committee must understand the interrelationships between the processes and systems
- A business process is a collection of tasks that produce a specific service or product for a particular customer or customers
    - For example if the organization determines that in Accounting System is a critical application and the Accounting System rel
    - Although restoring the entire database server form to restore the critical Accounting System might not be necessary at least one
- Workflow documents should be provided to the recovery plan committee for each business process
- When dealing with an event that either partially or fully destroys the primary facility the organization will need an alternative location from which to operate until the primary facility can be restored
- The DRP should define the alternative location how to bring the alternative location two full operation and how the organization
- Also the DRP should include details on the security controls that were used to the primary facility and guidelines on how to implemenr these same controls at the alternate location
- The most important factor in locating an alternate location during the development of the DRP is to ensure that the alternative location is not affected by the same disaster
- All the main factors that affect the selection of an alternative location include the following:
    - Geographic location
    - Organization needs
    - Location cost
    - Location’s restoration effort
- When testing an alternative location is a vital part of any DRP. The DRP should include instructions on when and how to periodically test alternate sites to ensure that the contingency facility is compatible with the primary facility.
- The alternate locations should include the following:
    - Hot Site: A leased facility that contains all the resources needed for full operation, including computers, raised flooring, full utilities, electrical and communication wiring, networking equipment, and UPSs
        - The only resource to be restored at the hot site is the org’s data, often only partially.
        - Although providing quickest recovery it is the most expensive and can be hard to manage if it includes proprietary software
    - Cold Site: A leased facility that contains only electrical and communication wiring, A/C, plumbing, and raised flooring.
        - A cold site takes much longer to restore. It is the least expensive and most difficult to test.
    - Warm Site: A leased facility that contains electrical and communications wiring, full utilities, and networking equipment.
        - In most cases, the only devices that are not included in a warm site are computers
        - A warm site is the most widely implemented
    - Tertiary site: A secondary backup site in case the Hot, Warm, Cold sites are unavailable
        - Tertiary sites protect against catastrophes that affect large geographic areas
- Alternative locations include the following:

    - Reciprocal Agreements: An agreement between two org's that have similar tech needs and infrastructure
        - Both orgs agree to act as an alternate location for the other if either of the orgs primary facilities are rendered unusable
        - In most cases, these agreements cannot be legally enforced
        - A disadvantage of this site is that it may not be able to handle the workload of the other org
    - Redundant Sites: a site that is identically configured as the primary site
        - A redundant or Mirrored Site is typically owned and not leased
        - Although they are expensive, many orgs today see them as necessary
- Organizations must ensure that any DRP's include guidelines and procedures for recovering supplies and technology
- The DRP should include vendor contact information if supplies and technological assets must be purchased
- The DRP must include recovery information on the following assets that must be restored:
    - Hardware backup: includes client computers, servers, routers, switches, firewalls, and any other hardware that is running on the org's network
        - The DRP must include guidelines on restoring the data on these devices and information about restoring manually if the systems are damaged or destroyed.
        - The recovery plan team must determine the amount of time that it will take the hardware vendors to provide replacements for any damaged hardware
        - Organizations might need to explore other options, including purchasing redundant systems and storing them at an alternative location in case vendors cannot respond in a timely manner.
    - Software backup: Includes the applications and software that need to be running on the device
        - All software that is backed up usually requires at least an OS. Also, it may be required to install data management software on the backup server
        - All installation media, service packs, and updates should be stored at the alternate location.
        - All licensing should be documented as part of the DRP
        - Finally, frequent backups of applications should be taken
        - Some organizations might protect against a vendor's demise and procure source code to avoid obstacles should a vendor experience a disaster or bankruptcy
    - Human Resources: An occupant emergency plan specifically addresses procedures for minimizing loss of life
        - The HR team is responsible for contacting all personnel. Contact information should be stored onsite and offsite
        - After the initial event is over, the HR team should monitor personnel morale and guard against employee stress and burnout during the recovery period
        - Any DRP should provide adequate periods of rest for any personnel involved
        - IT should include guidelines on how to replace any personnel that are disaster victims
        - The org should ensure that payroll and benefits remain available
        - Because it can be hard to secure funding, signed checks should be securely stored offsite
        - An executive succession plan should be in place to ensure the org can continue to operate
    - Supplies: Disasters can affect the ability to supply an org with needed resources like paper, cabling, or even water. Vital resources should be documented and contacts of vendors to obtain them including alternate suppliers
    - Documentation: The personnel involved must be able to complete the appropriate recovery procedures
        - Each dept within the org should be asked to decide what dept docs are needed for operation
        - This should be centralized onsite and a copy should be retained offsite
        - Specific personnel should be tasked with ensuring that these docs are created, stored, and updated

Data Recovery Terms

    - Data Recovery: The data is one of the most critical assets when recovering from a disaster
        - Operations should determine which data is backed up, how often, and backup method(s)

    - The BCP teams are primarily concerned that the backed-up data can be restored in a timely manner
    - Backup schemes include:
        - Full Backup: everything is backed up and the archive bit in each file is cleared
        - Incremental Backup: all files SINCE the last full backup or incremental backup
        - Differential Backup: all files SINCE the last full backup
        - Copy Backup: like a full backup without flipping archive bits
        - Daily Backup: uses timestamp on file to determine changes, sometime multiple daily occur
        - Transaction Log Backup: only occur when the transactions since the last full backup are critical
        - FIFO rotation scheme: the newest backup is saved to the oldest media; this does not protect against data errors
        - Grandfather/Father/Son rotation scheme: perhaps daily, weekly, and monthly. Each day a son advances to the father, each month a father advances to the grandfather
        - Electronic Vaulting: Copies files as modifications occur in real time
        - Remote Journaling: Copies the journal or transaction log offsite on a regular schedule in batches
        - Tape Vaulting: Creates backups over a direct communication line to an offsite facility
        - Hierarchal Storage Management (HSM): Stores frequently accessed data on faster media
        - Optical Jukebox: Stores data on optical disks and uses robotics to load and unload them as needed. This is ideal when 24/7 availability is required
        - Replication: Copies data from one storage location to another. Synchronous replication uses constant data updates to ensure that the locations are close to the same, whereas asynchronous replication delays updates to a predefined schedule.
        - High Availability: in data recovery is a concept that uses redundancy and fault tolerance
        - Redundant Array of Independent Disks (RAID): A hard-drive technology in which data is written across multiple disks in such a way that a disk can fail and the data can be made available from remaking disks in the array
        - Storage-Area Network (SAN): High capacity storage devices connected to high speed private networks using storage specific switches
        - Failover: The capacity of a system to switch over to a backup system
        - Failsoft: The capability to terminate non-critical processes when a failover occurs
        - Clustering: Refers to a software product that provides load balancing services. One instance of an application server acts as a master controller and distributes requests to multiple instances using round-robin, weighted round-robin, or least-connection algorithms
        - Load Balancing: Refers to a hardware product that uses Application Delivery Controllers (ADC) that support the same algorithms, but also use complex number crunching processes such as per-server CPU and memory utilization, fastest response times, and so on, to adjust the balance of the load. Load balancing solutions are a.k.a. farms or pools
- Personnel should be given the appropriate time and monetary resources to endure that adequate training occurs. This includes allowing personnel to test any DRPs
- Training should be obtained from both internal and external resources
- When job duties change or new personnel are hired, policies should be in place to ensure the appropriate transfer of knowledge occurs

Critical Terms and Duties

- After personnel health/safety and damage mitigation occur next comes disaster recovery

- During any disaster recovery, financial management is important. Financial management usually includes the CFO and any other key accounting personnel
  - This group must track the recovery costs and assess the cash flow projections
  - This group is responsible for establishing payroll continuance guidelines, procurement procedures, and emergency cost tracking procedures.
- Orgs must decide which teams are needed during a DR and ensure that the appropriate personnel are placed on each of these teams.
  - Damage Assessment Team: Responsible for determining the disaster's cause and amount of damage that has occurred to the org's assets. It identifies all affected assets and the critical assets' functions after the disaster and determines which assets need to be restored/replaced and contact the appropriate teams that need to be activated
  - Legal Team: Deals with all legal issues immediately following a disaster and during the disaster recovery and oversees any public relations events that are held to address the disaster. The legal team should be consulted to ensure that all recovery operations adhere to federal and state laws and regulations.
  - Media Relations Team: Informs the public and media whenever emergencies extend beyond the org's facilities according to the guidelines in the DRP. When issuing public statements, the media relations team should be honest and accurate about what is known about the event and its effects. A credible, informed spokesperson should deliver the org's response.
  - Recovery Team: Recovers the critical business functions at the alternative facility, mostly by ensuring that the physical assets are in place, including computers and other devices, wiring, and so on. The recovery team usually oversees the relocation and restoration teams.
  - Relocation Team: Oversees the actual transfer of assets between locations. This includes moving assets from the primary site and then returning those assets when the primary site is ready for operation.
  - Restoration Team: Ensures that the assets and data are restored to operations. The restoration team needs access to the backup media.
  - Salvage Team: Recovers all assets at the disaster location and ensures that the primary site returns to normal. The savage team manages the cleaning of equipment, the rebuilding of the original facility, and identifies any experts to employ in the recovery process. In most cases this team determines when operations can resume at the disaster site.
  - Security Team: Responsible for managing the security at both the disaster site and any alternate locations that the org uses during the recovery. They may need to hire outside contractors to aid in the process. Using contractors to guard the physical access to the site and internal resources to provide security inside is always better because the reduced state might make issuing the appropriate access credential to contractors difficult.

BCP Testing

- After the BPC is fully documented an org must ensure the plan is maintained
  - At a minimum, an org must evaluate and modify the BCP and DRP on an annual basis.
- Thorough testing, inaccuracies, deficiencies, and omissions are detected.
- Testing the BCP and DRP prepares and trains personnel to perform their duties. It also ensures that the alternative backup site can perform as needed
  - When testing occurs, the test is probably flawed if no issues with the plan are found.

- Checklist Test: Occurs when managers of each dept or functional area review the BCP. These managers make note of any modification to the plan. The BCP committee then uses all the management notes to make changes to the BCP.
- Table-Top Exercise: The most cost-effective and efficient way to identify areas of overlap in the plan before conducting higher level testing. A table-top exercise is an informal brainstorming session that encourages participation from business leaders and other key employees. In this exercise, the participants agree to a particular disaster scenario upon which they will focus.
- Structured Walk-Through Test: Involves representation of each dept or functional area thouroghly reviewing the BCP's accuracy. This type of test is the most importat test to perform prior to a live disaster.
- Simulation Test: The operations and support personnel execute the DRP in a role-playing scenario. This test identifies omitted steps and threats.
- Parallel Test: Validates the operation of a new system against its predecessor. The performance of the replacement system is compared to the primary system. If performance deficiencies are found, the BCP team researches ways to prevent these deficiencies from occurring.
- Full-Interruption Test: Involves shutting down the primary facility and bringing the alternative facility up to full operation. This is a hard switch-over in which all processing occurs at the primary facility until the switch is thrown. The test requires full coordination between all the parties and includes notifying users in advance of the planned test. An org should perform this type of test only when all other tests have been implemented are successful.
- Functional Drill: Tests a single function or department to see whether the function or department to see whether the function's DRP is complete. This type of drill requires participation of the personnel that perform the function.
- Evacuation Drill: Personnel follow the evacuation or shelter-in-place guideline for a disaster type. In this drill personnel must understand the area to which they are to report when the evacuation occurs. All personnel should be accounted for at that time.

BCP Testing

- After a test is complete, all test result should be documented, and the plans should be documented, and the plans should be modified to reflect those results.
- The list of successful and unsuccessful activities from the tests will be the most useful to management when maintaining the BCP.
- All obsolete information in the plan should be deleted, and any new information should be added.
- Modifying current information based on new regulations, laws, or protocols might be necessary.
- Version control of the plans should be managed to ensure that the org always uses the most recent version.
- The BCP should be stored in multiple locations to ensure that it is available if a location is destroyed by the disaster
- Multiple personnel should have the latest version to ensure that the plans can be retrieved if primary personnel are unavailable when the plan is needed.

Chapter 11 – Legal, Regulations, Investigations, and Compliance

Digital Crime

- An org usually adopts security practices that are driven by the laws and regulations from local, state, and federal gov't
- Even if the perpetrator is discovered, they cannot be held accountable if the investigation did not adhere to the law
- In the U.S.A., the Secret Service and the FBI share the task of investigating computer crimes
- Most security issues are perpetrated by employees; disgruntles employees pose the greatest threat
- The security prof's job is to ensure that all devices are updated in a timely manner and protected from internal and external attacks
- Security prof's must ensure that their orgs practice due care and due diligence as part of a comprehensive security plan
  - The org must provide a means for employees to report any incident or crime that they witnessed or are aware of while ensuring that employees feel safe doing so.
  - Mostly, employees do not want to report incidents because they do not want to be involved
  - There is also fear of being accused of something they did not do
  - Employees may not even be aware of the procedure to report a suspected crime
- Orgs should establish a culture that provides training and a means for reporting incidents
- Computer crimes today are usually made possible by a victim's carelessness
- Investigating and prosecuting computer crimes is difficult because the evidence if mostly intangible
- Obtaining a trail of the evidence activities is hard
- Security prof's should understand the following concepts:
  - Computer-Assisted Crime: occurs when a computer is used as a tool to commit a crime
    - When it can be committed without a computer but using a computer makes it easier
    - Criminals can steal org data without a computer
  - Computer-Targeted Crime: occurs when the computer is the victim and the purpose is to harm the computer and its owner
    - This cannot be carried out without a computer
    - Includes DoS and Buffer Overflow attacks
  - Incidental Computer Crime: when a computer is involved and without being the victim or the attacker
    - Perhaps a zombie in a botnet
  - Computer Prevalence Crime: occurs die to the fact that computers are so widely used today
    - Occurs only because computers exist
    - Key example is software piracy
- Hackers vs. Crackers: mistakenly interchanged
  - Hackers break into secure systems to obtain knowledge and use that for pranks or crimes
  - Crackers break into secure systems without any nefarious purposes
- Hat colors are more easily defined and understood:
  - White Hat: does not have malicious intent
  - Black Hat: has malicious intent
  - Gray Hat: often will exploit a vulnerability and notify the administrator to offer patching it for a fee.

Major Legal Systems

Civil Code Law: developed in Europe, it is based on written laws. It is a rule-based law that does not rely on precedence.

- The most common legal system in the world, it does not require higher and lower courts
- Do not confuse this with the US Civil/Tort laws

Common Law: developed in England and based on customs and precedents because no written laws were available

- It reflects the morals of the people and relies heavily on precedence; lower courts must follow higher court rulings
- In place today in the US, UK, Australia, and Canada
- Uses a jury based system, which can be waived and decided by a judge. Prosecution must provide proof beyond a reasonable doubt.
- Common Law has three systems:
    - Criminal Law: covers any actions that are considered harmful to others and conduct that violates public laws
        - Guilty parties may be fines and/or imprisoned
        - Based on common law and statutory law which is handed down from federal and state bodies.
    - Civil/Tort Law: the liable party owes a legal duty to the victim
        - The victim is entitled to compensatory, punitive, and statutory damages
            - Compensatory cover victim's losses
            - Punitive are punishments handles by juries
            - Statutory are based on damages established by laws
        - Includes economic damages, liability, negligence, nuisance, and dignitary torts
        - US civil law holds senior officials liable for civil wrongdoings by the org
    - Administrative/Regulatory Law: Standards of performance or conduct are set by the gov't to be followed
        - Common areas include public utilities, communication, banking, environmental protection and healthcare

Customary Law: based on the customs of a country or region

- Not typically used in isolation but used in many mixed law systems like African countries, China and Japan.
- Monetary fines or public service is the most common restitution for Customary Law.

Religious Law: based on religious beliefs

- Most are based on one religion; cultural differences exist country to country which effect enforcement

Mixed Law: Combines two or more of the other types; often used in civil law and common law

Intellectual Property Law: a group of laws that recognizes exclusive rights for creations of the mind

- It can be a tangible or intangible asset t which the owner has exclusive rights

Patent: granted to an individual or company to cover an invention that is described in the patent's application

- When granted, only the owner can make use of, or sell the invention for a period of time; usually 20 years
- Expiration means that the invention becomes public domain
- Many software companies fight legal battles over patents (MS, HP, Apple, etc.) which is why they employ legal teams to perform patent research before developing new technologies.
- Being first is considered crucial in today's highly competitive market.

Trade Secret: Ensures that proprietary technical or business information remains confidential

- Recipes, formulas, ingredient listings, etc.
- Once disclosed it is no longer considered a secret

- Most companies with trade secrets attempt to protect them with NDA's
- Anyone who signs an NDA will suffer legal consequences if violation can be proved

Trademark: Ensures that a symbol, sound, or expression is protected from being reused

- If not registered then an org should use a ™
- If it is registered then an org should use a ®

Copyright: Ensures that authored work is protected from reproduction or use without the consent of the copyright holder

- Lasts longer than a patent
- Many guidelines exist, but generally, anything after Jan 01, 1978 is the life of the author plus 70 years
- World Intellectual Property Organization (WIPO): in 1996 standardized the treatment of digital copyrights
- Copyright Management Information (CMI): is licensed ownership data that is added to any digital work.
- WIPO stipulates that CMI included in copyright material cannot be altered

Available Software Types:

- Freeware: Free to use, copy, modify, and distribute
- Shareware: Shared for a limited time
- Commercial Software: Licensed by a commercial entity

Software Piracy is unauthorized reproduction or distribution of copyrighted software

Proving Software Piracy encounters problems with cross-jurisdictional issues. It is difficult to get support from foreign agencies and gov'ts

Security Prof's and the orgs must ensure that the org takes measures to educate staff about installing pirated software

- Large orgs might need to utilize enterprise software to report on software installations

Employees are the greatest threat for any org

- Org's should take measures to protect confidential resources from unauthorized internal access
- Any info that is part of a patent, trade secret, trademark, or copyright should be given appropriate classifications
- Access controls should be customized for this information and audit controls should be implemented for access alerts
- Due Care procedures and policies must be in place to ensure that any laws that protect these assets can be used to prosecute an offender

Privacy

Privacy concerns cover three areas:

- Which personal information can be shared with whom
- Whether messages can be exchanged confidentially, and
- Whether and how one can send a message anonymously

As part of the security measures that orgs must take to protect privacy, Personally Identifiable Information (PII) must be understood, identified, and protected

Orgs must also understand privacy laws that governments have adapted, and comply with all privacy laws and regulations.

Personally Identifiable Information (PII)

- PII is any piece of data that can be used alone or with other data to identify a single person
- Any PII that an organization collects must be protected in the strongest manner possible

- Examples of PII include full name, identification numbers (i.e. SSN or Driver's license), date or place of birth, biometric data, account numbers, and digital denies like social media accounts
- Security Prof's must ensure that they understand international, national, state, and local PII regulations and laws
- Theft of this data is becoming more prevalent; more laws can be expected that will affect the security profession

Laws and Regulations

- Security Prof's must be aware of the laws and at least understand how they affect the operations at their orgs.
- Sarbanes-Oxley (SOX) Act: aka Public Company Accounting Reform and Investor Protection Act of 2002
  - Affects all publicly traded companies in the US
  - Controls accounting methods and financial reporting for he org and stipulates penalties and jailtime for execs
- Health Insurance portability and Accountability Act (HIPPA): aka Kennedy-Kassebaum Act
  - Affects all health care facilities, health insurance companies, and healthcare clearing houses
  - Provides standards for storing, using, and transmitting medical info and healthcare data
  - HIPPA overrides state laws unless the state laws are more strict
- Gramm-Leach-Bliley Act (GLBA) of 1999: Affects all financial institutions including banks, loan companies, insurance companies, investment companies, and credit card companies and provides guidelines for securing all financial information and prohibits sharing information with third parties
- Computer Fraud and Abuse Act (CFAA) of 1986: Affects any entity that might engage in hacking of protected computers as defined in the act
- It has been amended many times, most recently in 2008 by the Identify Theft Enforcement and Restitution Act
  - A protected computer is a computer used exclusively by a financial institution or the US gov't or used in or affecting interstate or foreign commerce or communication
  - This includes a computer located outside the US that is used in a manner that affects interstate or foreign commerce or communication in the US.
  - Due to the interstate nature of most internet communication, any ordinary computer/phone is under the jurisdiction
  - The law contains several definitions of hacking, including knowingly accessing a computer without authorization, intentionally accessing a computer to access financial records, US gov't information, or protected computer information, and transmitting fraudulent commerce communication with the intent to extort.
- Federal Piracy Act of 1974: Affects any computer that contains records used by a federal agency
  - It provides guidelines on collection, maintenance, use, and dissemination of PII
- Federal Intelligence Surveillance Act (FISA) 1978: Affects law enforcement and intelligence agencies
  - First act to provide guidelines/procedures for physical and electronic surveillance and collecting foreign intelligence between foreign powers and agents of foreign powers; but only applied to traffic in the US
  - It was amended by the USA PATRIOT Act of 2001 and FISA Amendments Act of 2008
- Electronic Communication Privacy Act (ECPA) of 1986: Affects law enforcement and intelligence agencies
  - It extended to gov't restrictions on wiretaps from phones to include transmission of electronic data
  - Amended by Communication Assistance to Law Enforcement Act (CALEA) of 1994, The USA PATRIOT Act of 2001 and the FISA Amendment Act of 2008
- Computer Security Act of 1987: Superseded by the Federal Information Security Management Act of 2002
  - To protect and defend any sensitive information of the federal gov't
  - Placed requirements on govt agencies to train employees and identify sensitive systems
- US Federal Sentencing Guidelines of 1991: Affects individuals and orgs convicted of felonies and serious (Class A) misdemeanors.
  - It stands to prevent sentencing disparities that existed across the US

- Communications Assistance for Law Enforcement Act (CALEA) of 1994: Affects law enforcement and intelligence agencies
    - Requires telecommunication carriers and manufacturers to modify the design to build in surveillance
    - This allows the deferral agencies to monitor all phone, internet and VoIP in real time.
- Personal Information Protection and Electronic Documents Act (PIPEDA): Affects how the private sector orgs collect, use, and disclose personal informatio in the course of commercial buseinss in Canada
    - The Act was written to address European Union (EU) concerns about PII security in Canada
    - It requires orgs to obtain consent to collect, use, or disclose personal info and to make the policies clear, understandable, and readily available.
- Basel II: affects financial institutions
    - It addresses minimum capital requirements, supervisory review, and market discipline
    - The main purpose is to protect against the risks the banks and other financial institutions face
- Payment Card Industry Data Security Standard (PCI DSS): affects any org that handles cardholder information
    - Latest version is 2.0
    - Annual review is required to prove compliance
- Federal Information Security Management Act (FISMA) of 2002: requires every federal agency to develop, document, and implement an agency-wide information security program
- Economic Espionage Act of 1996: affects orgs with trade secrets and people who plan to use encryption tech for criminal purposes; since this law theft of a trade secret is a federal crime.
- USA PATRIOT Act of 2001: affects law enforcement and intelligence agencies in the US
    - Enhances investigation tools for law enforcement to use with email, phone, internet communication, medical records, and financial records
    - Private citizens can use these tools to help when a warrant is needed, the government knows they are using them, or when acting as a government agent
- Health Care and Education Reconciliation Act of 2010: affects healthcare and educational orgs
    - Increased security for healthcare information
- Employee privacy issues must be addressed by all orgs to protect the org
- Employees must be given proper notice of any monitoring that may be used
- Monitoring must be applied in a consistent manner
    - A no-expectation-of-privacy policy should be signed by the employee after appropriate training
    - This policy should specifically describe any unacceptable behavior
- Companies should keep in mind that some actions are protected under the Fourth Amendment
- Security prof's and senior management should consult with legal counsel when designing and implementing any monitoring solution

European Union (EU)

- EU principles on privacy include strict laws to protect private data
- The EU's Data Protection Directive provides direction on how to follow the laws set forth in the principles
- The EU then created the Safe Harbor Privacy Principles to help guide US orgs in compliance with EU principles
- Guidelines include:
    - Data should be collected in accordance with the law
    - Personal data cannot be shared with another org without explicit permission from the individual
    - Transferring information can only occur if the sharing org has adequate security
    - Data should only be used for the purpose for which it was collected
    - Data should be used only for a reasonable length of time
- Safe Harbor vs. Data Haven
    - EU defines Safe Harbor is an entity that confirms to all requirements of EU Principles on Privacy

  - Data Havens are countries that fail to legally protect personal data with the aim to attract companies engaged in data collection
- The EU Electronic Security Directive defines electronic signature principles
  - A signature must be uniquely linked to a signer and to the data which it related; so subsequent data changes are detectable
  - The signature must be able to identify the signer
- Many orgs today develop trade relationships with orgs that are in other countries
- Orgs must be aware of the export and import laws of the countries of both the source and destination countries
  - Encryption is sometimes the most restricted tech noted in import/export laws
  - The US limits encryption export for National Security reasons, China and Russia limit import to keep the tech from their citizens
- Orgs that import/export should involve legal counsel to ensure all laws and regulations are followed
- Orgs must ensure that security prof's obtain proper training since laws and regulations are constantly being enacted
- Orgs should obtain proper legal counsel to protect against future prosecution for the org and senior management

Liability

- The status of being legally responsible to another entity because of your actions or negligence
- Because of new laws, orgs and senior management can no longer afford to turn a blind eye to security issues
- Due diligence and due care are related to liability
  - Due Diligence: means an org understands the security risk that it faces and is about gathering the information
    - Orgs must institute procedures to determine risk
    - Provides information necessary to ensure Due Care can be completed
    - Without Due Diligence, Due Care cannot occur
  - Due Care: means that the org takes all reasonable actions to prevent the issue or mitigate damages and is about action
    - Orgs must institute protections and procedures for all org assets, especially IP
    - Failure to meet minimum standards and practices is considered negligent
  - If an org does not act as a prudent person would then the org is negligent
  - Due Diligence will allow the recognition of risk
  - Due Care will implement plans to protect against the risk
- Negligence means an org was careless and an org or individual was injured; this serves as a basis for lawsuits
- Under the Principle of Culpable Negligence, senior management can be held liable for losses
- Penalties an org can accrue include civil (victim compensation) and criminal (fines and jailtime) penalties
- Proximate Cause is a term associated with negligence; it proves the injury was due to the negligence
- Downstream Liability: liabilities accrues through partnerships (example is protecting PII using technology and training staff)
- Hackers are most often interested in seeing how far their skills will take them
  - Security Prof's must ensure that they keep up with hackers and tools
  - Hackers can use Crack, John the Ripper, Nessus, Saint, Nmap, and L0phtCrack
  - Security Prof's use these in an ethical manner to perform internal penetration testing
- Third-party outsourcing is also a liability; partners are entrusted to protect using proper security measures to meet regulatory and legal compliance
- Contract and Procurement processes must be formalized
  - Orgs should establish procedures for managing and include all regulatory and legal requirements
  - Periodic reviews should occur to ensure that the entity is complying with the guidelines of the contract

Incidence Response

The beginning of any investigation

- After discovery, incident response personnel perform certain tasks
- During the entire incident response the must ensure proper procedures are followed to preserve evidence
- The team must have the procedures in place which must not hinder any forensic investigation
- Event vs. Incident
    - An event is a change of state that occurs
    - An Incident response focuses on negative events; a series of events that impact an orgs ops or security
- Events can only be detected if the org has established proper auditing and security monitoring mechanisms

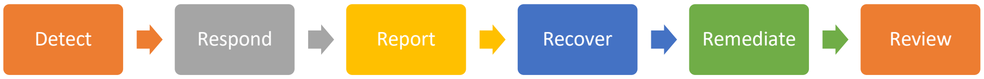
Incident Response Team and Incident Investigations

- Orgs must consider the technical knowledge of each team member
    - The team members must understand the orgs security policies and have strong communication skills
    - Members should also receive incident response and investigation training
- When an incident occurs the main goal is to contain the attack and repair any damage the incident caused
- Security isolation of an incident scene should start immediately when the incident is discovered
- Evidence must be preserved and appropriate authorities should be notified
- The team should have access to the Incident Response Plan
    - List of authorities to contact, team roles and responsibilities, internal contact list, securing and preserving evidence procedures, and a list of investigation experts that can help
    - Step-by-step manual should be created that the incident response team must follow
- After the process has been engaged all actions should be documented
- If the team determines that a crime has been committed, senior management and proper authorities should be contacted immediately

Rules of Engagement, Authorization, and Scope

- An org should document the rules of engagement, authorization, and scope for the response team
    - The rules need to define acceptable and unacceptable behavior
    - Authority and scope provide the team to perform their duties
- Rules of engagement act as a guideline for the team to prevent enticement (luring) or entrapment (when the individual is encouraged and had no intention of committing the crime).
- Enticement is legal but raises ethical arguments and may not be admissible in court. Entrapment is illegal.

Incident Response Procedures



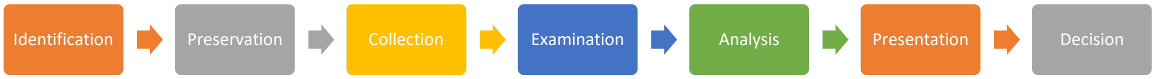
On Exam

- Investigation occurs during Respond, Report, and Recover
- Following the appropriate forensic guidelines ensures that evidence is preserved

Forensics and Digital Investigations

- Computer investigations require different procedures because timelines are compressed and experts may be required
    - Information is intangible and often requires extra care to retain data in the original format

    - The evidence of a computer crime is much more difficult to gather
- Standardized procedures should include the following:
    - Identify what type of systems is to be seized
    - Identify the search and seizure manner
    - Determine the risk that the suspect will destroy the evidence
- After law enforcement has been informed the orgs investigators' constraints are increased
    - Turning the investigation over to ensure evidence is preserved may be necessary
- When investigating a computer crime, evidentiary rules must be addressed
- Computer evidence should prove a fact that is material to the case, and it must be reliable
- The chain of custody must be **maintained** and **documented**; or it may not be admissible in court.
- Any forensic investigation involves the following steps:

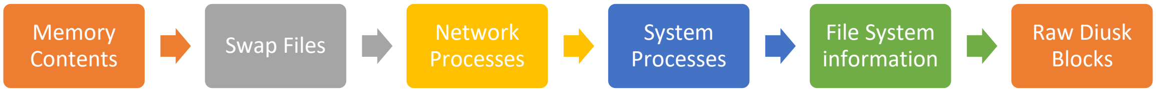


Step 1: Identify Evidence

- Identify and secure the crime scene and identify the evidence (i.e. audit logs, monitoring systems, user complaint reviews, and detection mechanisms)
- Preserving evidence you may not need is always better than wishing you preserved it later
- The attacked system is considered the crime scene
    - In some cases, the system that originated the attack can also be considered part of the crime scene
    - Fully capturing the attacker's system is not always possible
    - For this reason, you should capture any data that can point to a specific system (ex. IP, username, etc.)

Step 2: Preserve and Collect Evidence

- Preserving and collecting evidence includes system images, chain of custody, documenting and timestamping
- Before collecting evidence consider the order of volatility:



- Images must be made with a tool that creates a bit-level copy, which mostly requires isolating the system removing it from production
- Two copies should be retained
    - One stored for evidence
    - The other used for analysis
- Message digests should be used to ensure data integrity
- You might also want to assemble a field kit; commercial kits are available but org needs differ

Step 3: Network Processes

- While examining, any characteristics such as timestamps and ID properties should be determined and documented
- After the evidence has been fully analyzed using scientific methods, the full incident should be reconstructed and documented

Step 4: Present Findings

- Presenting findings in a format the audience can understand is best
- It is important that the expert articulate the details to a non-technical audience

Step 5: Decide

- At the end of the court proceeding, a decision will be made as to the guilt or innocence of the accused party
- At that time, evidence will no longer need to be retained
- Documenting lessons learned is important; anyone involved in the investigation should contribute to post-mortem
- International Organization on Computer Evidence (IOSC), and Scientific Working Group on Digital Evidence (SWGDE) both study digital forensics and help to establish standards for digital investigations
    - Both groups release guidelines about data on computers, phones, automobiles, and other devices
    - Any investigation should comply with the principles from these groups
- Main principles are:
    - The general rules of evidence should be applied to all digital evidence
    - Upon seizing digital evidence, actions taken should not change the evidence
    - When a person needs to access original digital evidence, that person should be suitably trained for that purpose
    - All activity relating to the seizure, access, storage, or transfer must be fully documented and available for review
    - An individual is responsible for all actions taken with respect to the evidence while in that individuals possession

Crime Scene

- A crime scene is the environment where potential evidence exists
- Once the scene is identified steps should be taken to ensure that the physical and virtual environments are protected
    - Physically, the system may need to be removed from the network
    - However, the system should NOT be powered down until all evidence has been captured
        - Live computer data is dynamic and is possibly stored in several volatile locations
- Access to the crime scene should be tightly controlled and limited to the only to individuals vital to the investigation
    - Document anyone who has accessed the crime scene
- Once a crime scene is contaminated, there is no method to restore it to the original condition.

MOM: Motive, Opportunity, and Means is the most basic strategy for determing suspects

- Motive is about why the crime was committed and who committed it
- Opportunity is about where and when the crime occurred
- Means is about how the crime was carried out by the suspect
    - Any suspect must meet all three criteria

Chain of Custody: shows who controlled, secured, and obtained the evidence

- A proper chain of custody must be preserved to prosecute a suspect
- Following the Chain of Custody means the evidence was collected following all predefined procedures and in accordance with al laws and regulations
- Primary purpose is to ensure that evidence is admissible in court
- Involving law enforcement early in the process can help ensure that the chain is followed

Interviewing: One person should be in charge of interviews

- Because evidence is being obtained, ensure the interviewer understands what information needs to be obtained and that all questions are important
- Reading a suspect Miranda Rights is ONLY necessary if law enforcement is performing the interview
- Recording is a good idea to provide corroboration later when the interview is used as evidence
- If an employee is suspected of a computer crime, HR should be involved in the interrogation
- The employee should be interviewed by an individual who is senior to that employee

Evidence: must be relevant, legally permissable, reliable, properly identified, and properly preserved

- Relevant means that it must prove a material fact related to the crime.
    - Shows a crime was committed,
    - Can provide information describing the crime,
    - Can provide information about motive, or
    - Can verify that the crime occurred
- Reliable means it has not been tampered with or modified
- Properly preserved means it is not subject to damage or destruction

All evidence must be tagged

- Evidence tags should document the mode and means of transportation, complete description including the quality, who receives it, and who had access to the evidence

Five rules of evidence:

1. Be authentic
2. Be accurate
3. Be complete
4. Be convincing
5. Be admissible

Types of evidence:

- Best Evidence: this rule states that only an original will be presented unless there is a legitimate reason
    - In most cases digital evidence is not best evidence because it is copied
    - Courts can apply best evidence rules on a case-by-case basis
    - In this case, a copy must be proved by an expert witness who testifies and confirms accuracy
- Secondary Evidence: has been reproduced or is substituted for the original item
    - Copies of original documents and oral testimony are considered secondary evidence
- Direct Evidence: Proves or disproves a fact through oral testimony based on the witness's senses
    - A witness can testify to what they saw, smelled, heard, tasted, or felt
    - Only a witness can provide direct evidence
    - If anyone else were to report these things it is called hearsay
- Conclusive Evidence: Does not require any other corroboration and cannot be contradicted by other evidence
- Circumstantial Evidence: provides inference of information from other intermediate relevant facts
    - Used to bring a jury to a conclusion by using a fact to imply that another fact is true or false.
- Corroborated Evidence: Supports another piece of evidence
- Opinion Evidence: based on what a witness thinks, feels, or infers.
    - If the witness is an expert, then they can testify on a fact based on knowledge and it is not opinion evidence
- Hearsay Evidence: secondhand; when the witness was told by someone else
    - In some cases, computer-based evidence is considered hearsay, especially if an expert cannot testify to the accuracy or integrity of the evidence

Surveillance, Search, and Seizure

- Surveillance: is the act of monitoring behavior, activities, or other changing information; usually people
    - Investigators use:
        - Physical: using cameras, direct observation, or CCTV

        - Computer: audit logs, key capture, etc.

- Search: is the act of pursuing items or information
    - A search warrant is required in most cases to search a private site for evidence
    - A search warrant is issued by a judge who is convinced that probable cause exists
    - No warrant is needed during exigent circumstances that are necessary to prevent physical harm, the evidence destruction, the suspects escape, or some other consequence improperly frustrating the effort
- Seizure: is the act of taking custody of physical or digital components
    - Only evidence specifically listed on the search warrant can be seized and the search can only occur in areas listed in the warrant
    - Search and seizure rules do not apply to private organizations and individuals
    - Most orgs warn staff that any files stored on org resources are considered property of the org

Media Analysis

The following types of media analysis can be used:

- Disk Imaging: creates an exact image of the hard drive contents
- Slack Space Analysis: analyzes the slack to determine if anything marked for deletion can be retrieved
- Content Analysis: Uses content to provide a report detailing types of data by percentage
- Steganography Analysis: Analyzes the files on a drive to see whether the files have been altered or to discover the encryption used on the file.

Software Analysis techniques:

- Content Analysis: analyzes content, particularly malware, to determine for which purpose the software was related
- Reverse Engineering: Uses source code to study how the program performs operations
- Author Identification: Attempts to determine the author
- Context Analysis: Analyzes the environment where the software was found to discover clues to determine risks

Network Analysis techniques:

- Communication Analysis: captures all or part of the communication and searches for particular types of activity
- Log Analysis: analyzes network traffic logs
- Path Tracing: tracing the path of a packet to discover the route used by the attacker

Hardware/Embedded Device Analysis: uses tools and firmware provided with the device to detemine what happened

- In most cases, the device vendor can provide advice on the best technique depending on the information you need
- Log analysis, OS analysis, and memory inspections are generally used

Security and Professional Ethics

- Ethics for any profession are the moral principle of that occupation
- Security Prof's should understand the ethics that are published by the (ISC)^2, the Computer Ethics Institute, the Internet Architecture Board (IAB), and their employer

(ISC)2 Code of Ethics provides a strict code for certification holders

- All cert holders must follow the Code of Ethics
- Any reported violations of the code are investigated
- Certificate holders who are found guilty of violation will have their certification revoked
- The four mandatory canons of certificate holders are:
    - Protect Society, the common good, necessary public trust and confidence, and the infrastructure

    - Act honorably, honestly, justly, responsibly, and legally
    - Provide diligent and competent service to principles.
    - Advance and protect the profession
- Any certificate holders are required to report any actions by other certificate holders that they feel are in violation
- If someone is reported, a peer review committee will investigate the actions and decide the certificate holder's standing
- A certificate holder must complete certain educational requirements to prove continued competence

Computer Ethics Institute has created the Ten Commandments of Computer Ethics:

- Do not use a computer for harm
- Do not interfere with the computer work of other people
- Do not snoop around in the computer files of other people
- Do not use a computer to steal
- Do not use a computer to lie
- Do not install and use licensed software unless you have paid for it
- Do not use another person's computer unless you have permission or have paid the appropriate compensation
- Do not appropriate another person's intellectual output
- Consider the consequences of the program you are writing or the system you are designing
- Always use a computer in ways that ensure consideration and respect of other people and their property

IAB: oversees the design, engineering, and management of the internet

- Ethics statements issued by the IAB usually detail any acts they deem irresponsible like:
    - Wasting resources
    - Destroying data integrity
    - Compromising privacy
    - Accessing resources that they are not authorized to access
- Request for Comments (RFC) 1087: called Ethics and the Internet is the specific IAB document that outlines unethical Internet behavior

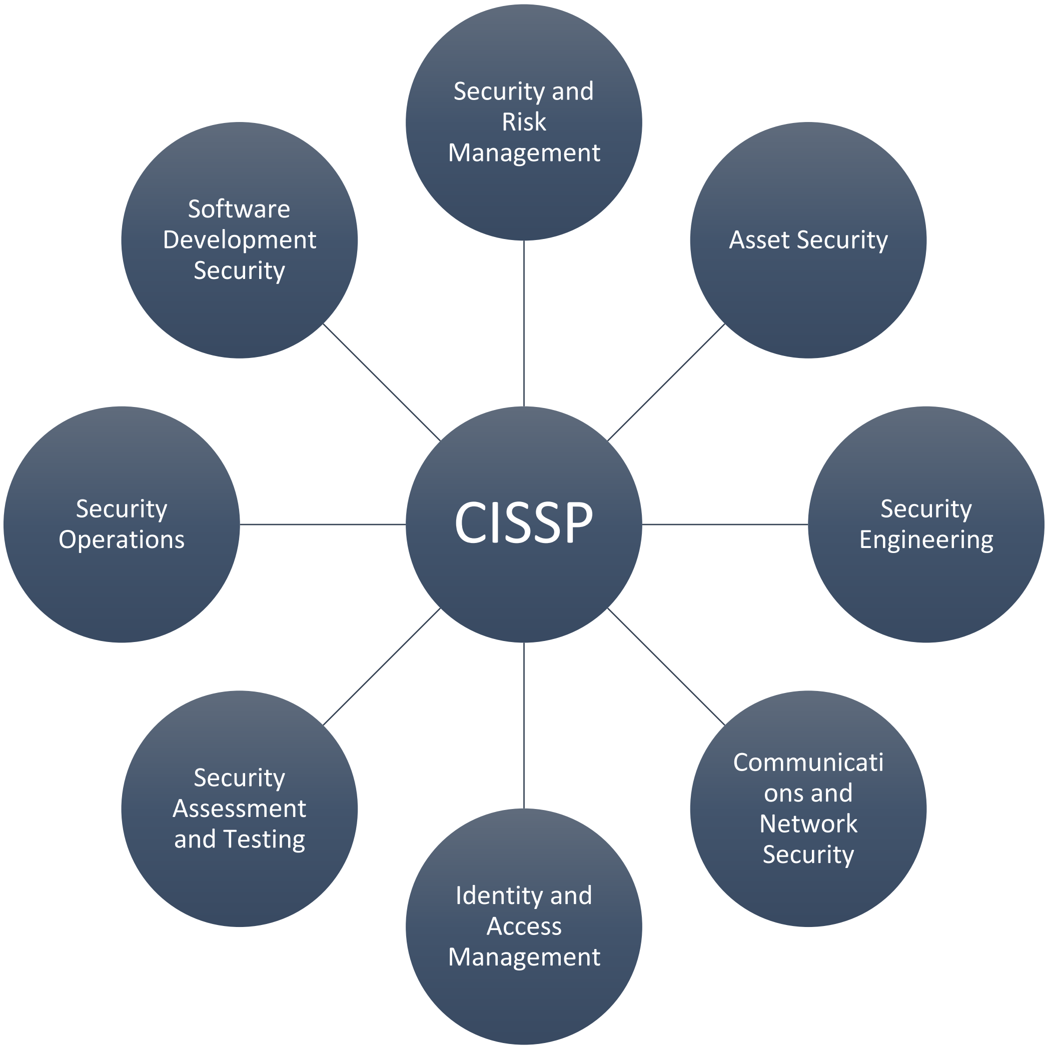
Organizational Ethics a formal program stresses to staff that they are expected to act in an ethical manner in all business dealings

- Several laws in the US can affect the development and adoption of an org ethics program
- If an org adopts an ethics program, the liability of the org is often limited, even when the staff are guilty of wrongdoing, provided the org ensures that personnel have been instructed on the org's ethics

Appendices

Used for documenting extra materials

Current CISSP Domains


Security and Risk Management
Asset Security
Security Engineering
Communications and Network Security
Identity and Access Management
Security Assessment and Testing
Security Operations
Software Development Security
CISSP