**Infosys 341 Exam Definitions**

# SESSION 2: Cryptography

* Cryptography: process of making and using codes to secure transmission of information
* Encryption: converting original message into a form unreadable by authorized individuals
* Decryption: The process of converting the ciphertext message back into plaintext
* Cryptanalysis: Process of obtaining original message from encrypted message without knowing algorithms
* Cryptology: science of encryption; combines cryptography and cryptanalysis.
* Key space: the entire range of values that can be sued to construct and individual key.
* Cipher Methods: block cipher or bit stream
  + Block: message divided into blocks using algorithm and key
  + Bit: each plaintext bit transformed into cipher bit one bit at a time.
* Substitution cipher: Sub one value for another
  + Monoalphabetic substitution: uses only on alphabet
  + Polyalphabetic substitution: uses two or more alphabets
  + Vigenere cipher: advanced cipher type uses simple polyalphabetic code; made up of 26 distinct alphabets
    - Method of encrypting alphabetic text by using a series of interwoven Caesar ciphers based on the letters of a keyword.
* Transposition Cipher: Rearranges values within a block to create ciphertext
  + Can be done at the bit level or at the byte level, keys and block sizes can be done much larger to make encryption stronger.
* Exclusive OR(XOR): function of Boolean algebra; two bits are compared
  + If two bits are identical, result is binary 0 else it is 1
  + Symmetric cipher
* Vernam Cipher: Uses set of characters once per encryption process
  + To perform:
    - The pad values are added to numeric values that represent the plaintext that needs to be encrypted
    - Each character of the plaintext is turned into a number and a pad value for that position is added
    - The resulting sum for that character is then converted back to a ciphertext letter for transmission
    - If the sum of the two values exceeds 26, then 26 is subtracted from the total.
* Book Cipher: Consists of a list of codes
  + Representing page number, line number, word number of the plaintext word
  + Looking up the references from the cipher text
  + Converts each reference to a word by using the ciphertext’s value and the key
* Hash Functions: Generate a message summary or digest to confirm identity/ integrity
  + Doesn’t use keys but has MAC, may be attached to a message (authenticate a message)
* Symmetric encryption: Uses same key to encrypt /decrypt
  + Data encrypted standard (DES) most popular symmetric encryption cryptosystems, 64-bit block size; 56-bit key
  + Triple DES(3DES): created to provide security far beyond DES
  + Advanced encryption standard (AES): developed to replace both DES and 3DES.
* Asymmetric encryption: uses two different but related keys
  + Either key can encrypt or decrypt message, if Key a encrypts message, only key B can decrypt
  + Highest value when one key serves as private key and the other serves as public key
  + RSA algorithm: was the first public-key encryption algorithm, used in web browsers to provide security for e-commerce applications.
* Public-Key Infrastructure (PKI)
  + Used to digitally sign documents transactions, and software to prove the source as well as the integrity of those materials.
  + Protects information assets in several ways:
    - Authentication, integrity, privacy, authorization, nonrepudiation (verifies message was sent by the sender)
* Digital signatures
  + Created in response to rising need to verify information transferred using electronic systems
  + Asymmetric encryption processes used to create digital signatures
* Digital certificates: electronic document containing key value and identifying information about entity that controls key.
* Diffie-Hellman Key exchange method: Most common hybrid system
  + Generating a shared secret key together.
  + Exchanging keys over a public channel
* Steganography: hiding information inside an image or audio file
  + Using the least significant bit, every byte is made up of 8 bits. However, not all of these 8 bits are necessary to define if a pixel of an image is red or white.
* Secure socket layer(SSL): uses public key encryption to secure channel over public internet
* Secure Hypertext transfer protocol (S-HTTP): extended version of hypertext transfer protocol: provides for encryption of individual message between client and server across internet.
* Secure Multipurpose internet mail extensions: based on asymmetric cryptography to protect your emails from unwanted access. It also allows you to digital sign your emails to verify you as the legitimate sender of the message.
* Privacy enhanced mail (PEM): Storing and sending cryptography keys, certificates and other data. Uses 3DES symmetric key encryption.
* Pretty Good privacy (PGB): Encryption program that provides privacy, authentication for data communication. Used for signing, encrypting and decrypting texts, e-mails, files etc.
* Secure electronic transactions: To provide protection from electronic payment fraud
  + Uses DES to encrypt credit card information transfers
  + Provides security for online and over the table payments.
* Wired equivalent privacy (WEP): provide data confidentially comparable to that of a traditional wired network.
* Wi-Fi protected access (WPA and WPA2): created to resolve issues with WEP
* Internet protocol security (IPSec): open source protocol to secure communications across any IP-based network
* IPSec designed to protected data integrity, user confidentially, and authenticity at IP packet level
  + Combination of several cryptosystems
* Man-in-the-middle Attack: Designed to intercept transmission of public key or insert known key structure in place of requested public key.
* Dictionary attacks: Attacker encrypts every word in a dictionary using same cryptosystem used by target
* Timing attacks: attacker eavesdrops during victim’s session
  + Uses statistical analysis of user’s typing patterns and inter-keystroke timings to discern sensitive session information

# SESSION 3: The Need for Security

* Business needs: Three business needs for an organization
  + Protecting the organization’s ability to function
  + Protecting the data and information the organization collects and uses
  + Safeguarding the organization’s technology’s assets in use.
* Threats: An object, person, or other entity that represents a constant danger to an asset
* Attack: An outgoing act against an asset that could result in a loss of its value
* Exploit: a vulnerability
* Threat agent: a person or other entity that may cause a loss in an asset’s value
* Intellectual property (IP): Ownership of ideas and control over the tangible or virtual representation of those ideas
* Software abuse organisations: Software and information industry association, business software alliance
* Malicious software (malware): Designed to damage, destroy, or deny service to target systems
  + Viruses: A type of malware that is attached to other executable programs. When activated, it replicates and propagates itself to multiple systems.
  + Worms: A type of malware that is capable of activation and replication without being attached to an existing program (host)
  + Trojan horses: A malware program that hides its true nature and reveals its designed behaviour only when activated.
  + Logic bombs: A set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.
  + Back door or trap door: A malware payload that provides access to a system by bypassing normal access controls.
  + Polymorphic threats: Threat evolves, changing, its size and other external file characteristics to elude detection by antivirus software programs.
* Quality of service: Situations where products or services are not delivered as expected
* Espionage or trespass: Unauthorized person gains access to information an organisation is trying to protect
* Competitive intelligence: Collection and analysis of information about an organizations business competitors (legal) – means of business intelligence and competitive advantage.
* Industrial espionage: Collection and analysis of information about an organizations business competitors (spying) illegal
* Shoulder surfing: covert observation of individual information or system use
* Expert hacker: uses extensive knowledge of the inner workings of computer hardware/software to gain unauthorized access to systems. Often create automated scripts.
* Unskilled hacker: uses the work of expert hackers to perform attacks. Include script kiddies and packet monkeys.
* Forces of nature: Present most dangerous threats because they usually occur with little warning and are beyond the control of people.
* Human error: Inexperience, improper training, incorrect assumptions. Employees are the greatest threats to an organization.
* Information extortion: The act of an attacker or trusted inside who steals information from a computer system and demands compensation for its return.
* Sabotage or Vandalism: Deliberate sabotage of a computer system or business
* Attacks: Acts or actions that exploits vulnerability in a controlled system
  + Malicious code: Includes execution of viruses, worms, Trojan horses, and active web scripts
  + Hoaxes: Transmission of a virus hoax with a real virus attached
  + Back door: gaining access to a system or network using known
  + Password crack: attempting to reverse calculate a password
  + Brute force: trying every possible combination of options of a password
  + Dictionary: selects specific accounts to attack and uses commonly used password to guide guesses
  + Denial-of-service: Attacker sends large number of connection or information request to a target
  + Distributed-denial-of-services: coordinated stream of requests to a target
  + Spoofing: techniques used to gain unauthorized access; intruder assumed a trusted IP address
  + Spam: Unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks
  + Mail bombing: also, a DoS; attacker routes large quantities of e-mail to target
  + Sniffers: Program or device that monitors data travelling over network; can be used both for legitimate purposes and for stealing information from a network
  + Phishing: an attempt to gain personal/financial information from individual, usually by posing as legitimate entity
  + Pharming: Redirection of legitimate web traffic to illegitimate site for the purpose of obtaining private information
* Software assurance: Is a methodological approach to the development of software that seeks to build security into the development life cycle rather than address at it later stages.
* Software design principles: Common place security principles:
  + Keep design simple and small
  + Access decisions by permission not exclusion
  + Every access to every object checked for authority
  + Design depends on possession of keys/passwords
  + Protection mechanisms require two keys to unlock
  + Programs/users utilize only necessary privileges
  + Minimize mechanisms common to multiple users
  + Human interface must be easy to use so users routinely/automatically use protection mechanisms

# SESSION 4: Legal, Ethical, and professional issues in Information Security

* Laws: Rules that mandate or prohibit certain societal behaviour
* Ethics: define socially acceptable behaviour
* Cultural mores: Fixed moral attitudes or customs of a particular group; ethics based on these.
* Due care: Insuring that employees know what constitutes acceptable behaviour and know the consequences of illegal or unethical actions
* Due diligence: Making a valid effort to protect others; continually maintaining level of effort
* Jurisdiction: A court’s right to hear a case if a wrong is committed in its territory or involves its citizenry
* Liability: The legal obligation of an entity that extends beyond criminal or contract law
* Long-arm jurisdiction: right of any court to impose its authority over an individual or organization if it can establish jurisdiction.
* Restitution: compensate for wrongs committed by an organization or its employees.
* Policies: Managerial directives that specify acceptable and unacceptable employee behaviour in the workplace
* Criteria:
  + Dissemination (distribution): The organization must be able to demonstrate that the relevant policy
  + Review (reading): The organization must be able to demonstrate that it disseminated the document in an intelligible form
  + Comprehension (understanding): The organization must be able to demonstrate that it disseminated the document in a intelligible form.
  + Uniform environment: The organization must be able to demonstrate that the policy has been uniformly
* Types of law:
  + Civil: Governs nation or state
  + Criminal: Addresses violations harmful to society actively enforced by the state
  + Private: Regulates relationships between individuals
* Computer crime laws:
  + Computer Fraud and Abuse Act of 1986 (CFA Act):
    - Corner stone of many computer-related federal laws and enforcement efforts
    - National information infrastructure Protection act of 1996:
      * Modified several sections on the previous act and increased the penalties for selected crimes.
* Privacy: Is a state of being free from unsanctioned intrusion
* Identity theft: Attempts to instigate penalties for identity theft by recognizing people who lose their identity as the true victims.
* NZ Privacy act:
  + Personal information is only to be collected for a lawful purpose connected with a function or activity of the agency
  + Information should be collected directly from the individual concerned and should be aware about this
    - The purpose for which the information is being collected
    - Who are the intended recipients
    - The consequences for the individual if the information is not provided
* Health and insurance portability and accountability act of 1996 (HIPAA)
  + Protects the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange
  + Consumer control of medical information
  + Boundaries on the use of medical information
  + Accountability for the privacy of private information
* Copyright Law
  + Intellectual property recognized as protected asset in many countries, like: NZ, AUS, USA; copyright law extends to electronic formats
* Financial reporting (Sarbanes – Oxley Act of 2002)
  + Seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies.
* State and local Regulations
  + Information security professionals must understand state laws and regulations and ensure that their organizations security policies and procedures are in compliance.

# SESSION 5: Planning for Security

* Governance: Set of responsibilities and practices exercised by the board and executive management
  + Goal to provide strategic direction, establishment of objectives, and measurement of progress towards objectives
  + Validates that risk management practices are appropriate and assets used properly
  + Five goals:
    - Strategic alignment
    - Risk management
    - Performance measures
    - Value delivery
    - Resource management
* Foundation for planning:
  + Policy: Sanctioned by management
  + Standards: Detailed minimum specifications for compliance
  + Guidelines: Recommendations for compliance
  + Procedures: Step-by-step instructions for compliance
* Enterprise information security policy: Sets strategic direction, scope, tone for all security efforts within a company
  + Executive level document usually draft by Chief Information officer (CIO)
  + Ensures meeting of requirements to establish program and assigning responsibilities
  + Use of specified penalty and disciplinary action
  + EISP should include:
    - Overview of corporate security philosophy
    - Responsibilities for security shared by all members and for each unique role.
* Issue-Specific Security Policy
  + The ISSP:
    - Addresses specific areas of technology
    - Requires frequent updates
    - Contains statement on the organization’s positions on specific issue
    - Three common approach’s when creating/manging ISSPs:
      * Create several independent ISSP documents
      * Create a single comprehensive ISSP document
      * Create a modular ISSP document
* Systems-Specific Policy
  + SysSPs often function as standards or procedures used when configuring or maintain systems
  + Systems-specific policies fall into two groups:
    - Managerial guidance
    - Technical specifications
* Policy management: Policies must be managed as they constantly change
  + Security policies must have:
    - A responsible manager
    - Schedule of reviews
    - Method for making recommendations for reviews
    - Policy issuance and revision date
    - Automated policy management
* Information Security Blueprint
  + Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls
  + Detailed version of security framework
  + Specifies tasks and order in which they are to be accomplished
  + Scalable, upgradable, and comprehensive plan for the current and future information security needs.
* ISO 27000 series : most common security model
  + Frame for IS that states companies security policy is needed to provide management direction and support
  + Purpose is to give recommendations for IS management and provides a starting point for developing organizational security.
* Design of Security Architecture
  + Spheres of security: foundation of the security framework
  + Levels of controls
    - Management controls set the direction and scope of the security processes and provide detailed instructions for its conduct.
    - Operational controls address personnel and physical security, and the protection of production inputs/outputs.
  + Organizations should establish multiple layers of security, controls and safeguards.
  + Security perimeter is pretty much an internal system protector from outside threats but it doesn’t take into account the onsite threats from employees
* SETA (Security education training awareness program)
  + SETA is a control measure designed to reduce accidental security breaches.
  + Improves awareness and builds in-depth knowledge.
  + Security education: everyone in an organization needs to be trained and aware of IS
  + Security training: Provides members of the organization with detailed information and hands on instruction to prepare them to perform their duties securely.
  + Security awareness: Designed to keep information security at the forefront of users minds
* Incident response plans (IRPs)
  + IRP focuses on immediate response; if attack escalates or is disastrous, process changes to disaster recovery and BCP
* Disaster recovery plans (DRPs)
  + DRP focuses on immediate response on restoring systems after disasters occur; as such, it is closely associated with BCP
  + Must decide which actions constitute disasters and which constitute incidents
  + Strives to re-establish operations at the primary site.
* Business continuity plans (BCPs)
  + BCP occurs concurrently with DRP when damage is major or ongoing, requiring more than simple restoration of information and information resources.
  + Prepares organization to relocate critical business operations during a disaster that affects operations at the primary site.
  + Must have a plan for businesses to “continue” functioning
  + Continuity strategies:
    - Hot sites: Has all the equipment needed for the enterprise to continue operation (office space, furniture etc)
    - Cold sites: Is an office but doesn’t necessarily have all the equipment needed to continue operation. Takes longer than a warm site and cold site to set up but is the cheapest option out of the three. Contains basic technical facilities
    - Warm sites: cheaper move from a hot site but only contains power, phone network etc may have servers.
* Contingency Planning (CP) process:
  + Come back to this
* Business impact analysis (BIA):
  + Investigation and assessment of various adverse events that can affect organization
  + Assumes security controls have been bypassed, failed, or proven ineffective and attack has succeeded.
  + Determine mission/business processes and recovery criticality
  + Identify recovery priorities for system resources
  + Identify resource requirements
* Incident Response Planning:
  + Incident response planning includes identification/classification of an response to a incident. Companies ability to respond to a security incident.
  + Attacks classified as incidents if they:
    - Are directed against information assets
    - Threatens CIA of information resources.
  + Incident planning:
    - Predefined responses enable the organization to react quickly and effectively to detected incident if:
      * The organization has an IR team
      * The organization can detect the incident
    - IR team consist of individuals needed to handle systems as incident takes place.
  + Incident detection:
    - Most common occurrence is complaint about technology support
    - Training needed to identify and classify an incident
  + Incident reaction
    - Consists of actions that guide the organization to stop incident, mitigate its impact, and provide information for recovery.
  + Incident containment strategies
    - Containment of incidents scope or impact as priority; must then determine which information systems are affected
  + Incident recovery
    - Once incident has been contained and control of systems regained, the next stage is recovery
  + Damage assessment
    - Several sources of information on damage can be used, including system logs, intrusion detection logs, configuration logs, and documents, documentation from incident response, and results of detailed assessment of systems and data storage.
  + Automated response
    - New systems can respond to incident threat autonomously
    - Ethical issues, legal abilities of a counterattack

# SESSION 6: Security technology: Firewalls an VPNs

* Access control: Method by which systems determine whether and how to admit a user into a trusted area of the organization
  + ITSEC: an international set of criteria for evaluating computer systems, compares targets of evaluation to detailed security function specifications
  + Bell-LaPadula Confidentiality model: Mode of an automated system able to manipulate its state or status. Focuses on data confidentiality.
  + Bib integrity model: Based on the premise that higher levels of integrity are more worthy of trust than lower ones. The intent is to provide access controls to ensure that objects or subjects cannot have less integrity as a result of read/write operations.
    - The model ensures that no information from a subject can be passed on to an object in higher level in order to prevent contaminating data of high integrity with data of lower integrity.
  + Clark-Wilson Integrity model: Built on change control rather than integrity levels, was designed for the commercial environment. The model’s change control principles are:
    - No changes by unauthorized subjects
    - No unauthorized changes by authorized subjects
    - Maintenance of internal and external consistency
      * Internal consistency means that the system does what it is expected to do every time, without exception
      * External consistency means that the data in the system is consistent with similar data in the outside world.
  + Brewer-Nash Model: Designed to prevent conflict of interest between two parties
* Mandatory access control (MACs): Use data classification schemes
* Discretionary access controls (DACs): Allow users to control and possibly provide access to information / resources at their disposal.
  + Controlled by user
* Nondiscretionary controls: strictly enforced version of MACs that are managed by a central authority.
  + Controlled by organization.
* Identification:
  + Authentication: the process of validating a supplicant’s purported identity
  + Authentication factors (something a supplicant knows) such as a password or passphrase. Or it can be something they carry such as physical characteristics
* Authorization: The matching of an authenticated entity to a list of information assets and corresponding access levels
  + Authorization for each authentication user
  + Members of a group
  + Across multiple systems
* Accountability: Ensures that all actions on a system = authorized or unauthorized – can be attributed to an authenticated identity.
* Biometrics: Approach based on the use of measureable human characteristics/traits to authenticate identity.
  + Trusted computing base: The trusted computing base (TCB) is everything in a computing system that provides a secure environment. Includes the OS and its provided security mechanisms, hardware, physical locations, network hardware and software mechanisms.
  + Biggest challenges include covert channels
    - Covert channel is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.
      * Storage channels: Which are used in steganography
      * Timing channels: which are used in a system that places a long pause between packets to signify a 1 and a short pause between packets to signify a 0.
* Firewalls: Prevent specific types of information from moving between an untrusted network (the internet) and a trusted network ( organization’s internal network)
  + Separate computer system
  + Software service running on existing router or server
  + Separate network containing supporting devices
  + Firewall filters only have two parameters (address of message where it comes from and what sort of service it is/provides).
  + Processing modes by which firewalls can be categorized:
    - Packet filtering: Examines the header information of data packets
      * Based on the combination of:
        + IP source and destination address
        + Direction (inbound or outbound)
        + Transmission control protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests.
      * Types of filtering firewalls:
        + Static filtering: Requires that filtering rules be developed and installed within the firewall
        + Dynamic filtering: Allows firewall to react to emergent event and update or create rules to deal with event
        + Stateful inspection: firewalls that keep track of each network connection between internal and external systems using a state table.
    - Application gateways:
      * Application layer firewall: frequently installed on a dedicated computer; also known as a proxy server.
      * Since proxy server is often placed in unsecured area of the network, it is exposed to higher levels of risk from less trusted networks.
    - Circuit gateways
    - MAC layer firewalls
      * Designed to operate media access control sublayer of network’s data link layer
      * Make filtering decisions based on specific host computer’s identity.
    - Hybrids
      * Combine elements of other types of firewalls, that is elements of packet filtering, and proxy services, or of packet filtering and circuit gateways.
* Firewall architectures
  + Common architectural implementations of firewalls:
    - packet-filtering routers
      * They can be configured to reject packets that the organization doesn’t allow in the network
    - dual-homed firewalls (bastion hosts)
      * Commonly referred to as sacrificial host, as it stands as sole defender on the network perimeter
      * Contains two network interface cards (NICs): one connected to external network and one connected to internal network
      * Implementation of this architecture often makes use of network address translation
    - screened host firewalls
      * Used to separate components of the firewall onto separate systems, thereby achieving greater throughput and flexibility, although at some cost to simplicity.
    - screened subnet firewalls
      * Protects DMZ systems and outside threats
      * Protects internal networks by limiting how external connections can gain access to internal systems
* Content filters
  + Software filter: not a firewall, allows administrators to restrict content access from within a software
  + Primary purpose to restrict internal access to external material
* Virtual Private Networks (VPNs)
  + Private and secure network connection between systems; uses data communication capability of unsecured an public network
  + Three VPN techs defined:
    - Trusted VPN
    - Secure VPN
    - Hybrid VPN
  + VPN must accomplish:
    - Encapsulation of incoming and outgoing data
    - Encryption of incoming and outgoing data
    - Authentication of remote computer and perhaps remote user as well
      * It allows the user to turn internet into private network.
    - Transport mode
      * Data within IP packets is encrypted ,but header information is not.

# SESSION 7: Risk Management

* Risk: The probability of a successful attack on the organization
  + Loss frequency = likelihood \* attack success probability
* Risk Management: The process of identifying, assessing, and reducing risks facing an organization.
* Risk identification: The enumeration and documentation of risks to an organization information asset. What can go wrong
* Risk control : The application of controls that reduce the risk to an organization’s asset to an acceptable level. The damage
* Risk assessment: Determine loss frequency, evaluate loss magnitude, calculate risk. What can happens
  + Evaluates the relative risk for each vulnerability
  + It assigns a risk rating or score to each information asset
  + Planning and organizing risk assessment
    - The goal at this point is to create a method for evaluating the relative risk fo each listed vulnerability
* Risk appetite and Residual Risk
  + Risk appetite it defines the quantity and nature of risk that organizations are willing to accept as trade-offs between perfect security and unlimited accessibility.
  + Residual risk: risk that has not been completely removed, shifted, or planned for
    - The goal of Information Security is to bring residual risk into line with risk appetite.
* Loss frequency: Likelihood of an attack combined with expected probability of success
  + Use external reference for values that have been reviewed / adjusted for your circumstances
* Transference: Strategy attempts to shift risk to other assets, processes, or organizations
* Acceptance: Doing nothing to protect a vulnerability and accepting the outcome of its exploitation
  + Valid only when the function, service, information, or asset does not justify the cost of protection.
* Termination: Directs the organization if an alternative being evaluated is worth the cost incurred to control vulnerability.
* Cost benefit analysis (CBA) formula
  + CBA determines if an alternative being evaluated is worth the cost incurred to control vulnerability
    - The CBA is most easily calculated using the ALE from earlier assessments, before implementation of the proposed control:
      * CBA = ALE(prior) – ALE(post) – ACS
    - ALE(prior) is the annualized loss expectancy of risk before implementation of control
    - ALE(post) is the estimated ALE based on control being in place for a period of time
    - ACS is the annualized cost of the safeguard
* Benchmarking: Process of seeking out and studying practices in other organizations that one’s own organization desires to duplicate
* Baselining: Comparing what your company is doing with another company
* Maybe add stuff about feasibility studies?

# SESSION 8: Intrusion detection and prevention systems, and other security tools

* Alarm clustering compaction: Cluster attacks into specific groups
* Confidence value: Describe what trust we have in the intrusion detection system
* Evasion: if we can somehow eliminate the possible bad influence of the attack
* False attack stimulus: are a way of testing the system of some sort of attack to see how the system reacts to this abuse.
* False negative – important factor, we are being attacked successfully but we are getting no information about it.
* Noise: We may be subject of permanent attack, they may be weak. We know about the attack, but we can sustain the attack. We can filter those attacks as low-level attacks which are called noise.
* Site policy: Which way we deploy our Intrusion detection system, set up settings of these systems
* Site policy awareness: People need to know what sort of measure we have implemented
* True attack stimulus: Testing our system against given type of attack (pen testing, penetration testing)
* Tuning: set up all the parameters of intrusion detection carefully
* Intrusion detection: primary purpose to identify and report intrusion, contain an attack and prevent the loss or damager.
* Network based: is a system to monitor network as well as protect the CIA of a network. Its main functions include protecting the network from threats, such as Dos and unauthorized usage.
* Wireless based: Same as network based but focuses on wireless network traffic.
* Host based: Resides on a computer or server (host) and monitors activity only on that system
* Signature based: Examines network traffic in search of patterns that match known signatures, used a lot because many attacks have clear and distinct signatures.
* Anomaly based: Collects statistical summaries by observing traffic known to be normal, when measured activity is outside the baseline parameters or clipping level, IDPS sends an alert to the administrator.
* Stateful protocol analysis: Process of comparing known normal protocol profiles against observed traffic, stores and uses relevant data detected in a session to identify intrusions involving multiple requests/responses.
* Active response: collecting additional information about the intrusion, modifying the network environment, and acting against the intrusion.
* Passive response: Setting off alarms or notifications, and collecting passive data through SNMP traps (alert messages).
* Deployment and implementation: An IDPS can be implemented via one of the tree basic control strategies:
  + Centralized: all IDPS control functions are implemented and manage in a central location
  + Fully distributed: all control functions are applied at the physical location of each IDPS component
  + Partially distributed: combines the two, Individual agents can report to a hierarchical central facility to enable organization to detect widespread attacks.
  + NIST recommends four locations for NIDPS sensors:
    - Location 1: Behind each external firewall, in the network DMZ
    - Location 2: Outside an external firewall
    - Location 3: On major network backbones
    - Location 4: On critical subnets
* Honeypots: Decoy systems designed to lure potential attackers away from critical systems
  + Several honeypots connected on a network segment.
  + They are designed to:
    - Divert an attacker from accessing critical systems
    - Collect information about the attacker’s activity
    - Encourage the attacker to stay on a system long enough for administrators to document the event and perhaps respond.
  + Padded cell system: protected honeypot that cannot be easily comprised
* Footprinting: Process of collecting publicly available information about a potential target.
* Fingerprinting: systematic survey of target organization’s internet addresses collected during the Footprinting phase to identify network services offered by hosts in that range.
  + Reveals useful information about the internal structure and nature of the target system or network to be attacked
* Port scanners: Tools used by both attackers and defenders to identify/fingerprint computers active on a network and other useful information.
* Vulnerability scanners: Examine the networks for detailed information and initiate traffic to determine security holes, listen on network and find problems with the server and client software.
* Packet sniffers: Captures copies of packets from network and analyses them. Needs to be under direct authorization of owners of the network to be used legally.

# SESSION 9: Physical Security

* Seven major sources of physical loss: Extreme temperature, gases, liquids, living organisms, projectiles, movement.
* Physical security controls: Walls, guards, dogs, locks and keys, mantraps, electronic monitoring, alarms and alarm systems.
  + ID cards: server as a simple form of biometrics (facial recognition) Tailgating can occur
  + Locks and keys
    - Two types of locks: mechanical and electromechanical
    - Locks can also be divided into four categories: manual, programmable, electronic biometric.
    - Locks fail in one of two ways:
      * Fail-safe locks are unlocked when the power goes out
      * Fail-secure locks are locked when the power goes out
  + Mantraps: small enclosure that has an entry point and a different exit point
    - Individual enters mantrap, request access and if verified can exit mantrap into facility.
  + Electronic monitoring: includes cameras CCTV etc.
* Fire suppression: Systems can consist of portable, manual or automatic apparatus
  + Portable extinguishers are rated by the type of fire: Class A, Class B, Class C, Class D, Class K.
  + Class A – fire at home (paper, carton, timber)
  + Class B - liquid, petrol on fire
  + Class C- If given device is connected to electricity

# SESSION 10: Physical Security

* Digital forensics: The science of identifying, preserving, recovering, analysing and presenting facts about digital evidence found on computers or digital storage media devices.
* Acquisition: search warrant and search order (execution is the same but search warrant is issued by high court judge.
* FTK: Index’s whole file, simply searches the index and provides the answer very quickly
* Search warrant: court order that a judge issues to authorize law enforcement officers to conduct a search of a person for evidence of a crime.
  + Scope of the warrant – Must be clearly defined
  + Legal privilege issues
  + Impact on the running of the business
* Expert witness: Must have read agreed to the high court of conduct for expert witnesses
  + May give an “opinion” in evidence
  + Is there to assist the court
  + They are allowed to formulate this opinion; this opinion must only state the facts and not be bias.
* Qualifications, training, experience and ethics
  + Must have:
    - Formal qualifications (degrees)
    - Training certificates encase and FTK
    - Wide and detailed experience in IT industry
    - Legal procedure understanding
    - Business experience
    - Personal integrity
    - Credibility as an expert witness (professional indemnity insurance)

# SESSION 11: Security and Personnel

* Chief information security officer (CISO):
  + Top information security office; frequently reports to chief information officer
  + Manages the overall information security program
  + Drafts or approves information security policies
  + Works with CIO on strategic plans
  + Develops information security budgets
  + Sets priorities for purchase/implementation of information security projects and technology
  + Makes recruiting, hiring and firing decisions or recommendations
* Security manager:
  + Accountable for day-to-date operation of information security program
* Security technician:
  + Technically qualified employees tasked to configure security hardware and software
  + Tend to be specialized
* Background checks: Investigation into a candidates’ past should be conducted before organization extends offer to a candidate
  + Background check differ in the level of detail and depth with which a candidate is examined.
* Termination: Many organizations use an exit interview to remind former employee of contractual obligations and to obtain feedback
  + Security issues arise as employees leave an organization.
  + Employee collects all belongings and surrenders all keys, key cards, and other company property.
* Job rotation: employees know each other’s job skills
* Privacy: Organizations required by law to protect sensitive or personal employee information

# SESSION 12: Handling Cyber Warfare

* War definition:
  + War is a state of armed conflict between societies. It is generally characterized by extreme aggression, destruction, and mortality.
* Cyber war: Conflict in which digital technology plays an important role
* Moonlight Maze: Was the codename assigned to a series of attacks against the pentagon, NASA, United States department of energy and a range of research organisations that were identified in March 1998.
* Stuxnet: Stuxnet was a worm which targeted semens SCADA control systems the worm escaped its original target due to an error in its updating code.
* Gaza offensive: January 2009 major DDoS attack against Israeli internet infrastructure. The attack involved over half a mission computers.
* Ukraine: Cyber-attacks against Ukraine in 2014 were attributed to a Russian hacker grouped backed by the Russian government.
* USA: John Brennan, the CIA director, had his personal email hacked which had personal documents in it.
* 2016: DDoS attacks launched targeting systems operated by DNS provider Dyn, which caused major internet platforms and services to be unavailable to large swathes of users in America and Europe.
* 2017: Ransomware attack Petya hit large companies across 65 countries in two days.
* Why cyber war: Existence of low cost attack tools, relatively safe of the attackers. Identity of the attacker is difficult to establish.
  + Speed of attacks
  + Lack of implementation of effective security measures
  + Growth of numbers of individuals, groups, organisations ready to apply their protest.
* Target of cyber-attacks:
  + Critical infrastructure
    - Electric power production and distribution
    - Gas production and distribution
    - Water supply
    - Air traffic control
    - Road control