Developing Secure Information Systems:- Developing Secure Information Systems requires addressing a number of issues in **data security**, **network security** and **physical security**.

Data Security:- data security is the practice of keeping data protected from corruption and unauthorized access.

Network Security:- Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network accessible resources. Network security components often include:

- Anti-virus and anti-spyware
- Firewall to block unauthorized access to your network
- Intrusion prevention systems (IPS), to identify fast-spreading threats.
- Virtual Private Networks (VPN) to provide secure remote access.

Physical Security:- Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage. Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance etc.

Application Development Security:- Applications with vulnerabilities that are used by attackers to gain access the client-side applications. From there any number of things can happen. They can:

- Deface a web site
- Insert spam links directing visitors to another site
- Insert malicious code that installs itself onto a visitor's computer
- Insert malicious code that steals session IDs (cookies)
- Steal visitor information
- Steal account information
- Steal information stored in the database

Information Security Governance & Risk Management:-

Information Security Governance:- Information security governance is the system by which an organization directs and controls. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Governance ensures that security strategies are aligned with business objectives and consistent with regulations.

The five general governance areas are:

- Govern the operations of the organization and protect its critical assets
- Protect the organization's market share and stock price
- Govern the conduct of employees (technology resources, data handling, etc.)
- Protect the reputation of the organization
- Ensure compliance requirements are met

Characteristics of effective security governance:-The eleven characteristics of effective security governance are critical for an effective enterprise information security information program. They are:

- It is an institution wide issue
- Leaders are accountable
- It is viewed as an institutional requirement (cost of doing business)
- It is risk based
- Roles, responsibilities and segregation of duties are defined
- It is addressed and enforced in policy
- Adequate resources are committed
- Staff are aware and trained
- A development life cycle is required
- It is planned, managed, measureable and measured
- It is reviewed and audited

An effective information security program requires the development and maintenance of:

- A long-term information security strategy
- An overarching institutional security plan (which may be supported by underlying academic/administrative unit security plans and security plans for individual systems)
- Security policies, procedures, and other artifacts
- The system architecture and supporting documentation

Benefits of information security governance :-

- Increased predictability and reduced uncertainty of business operations
- Protection from the potential for civil and legal liability
- Structure to optimize the allocation of resources
- Assurance of security policy compliance
- Foundation for effective risk management.
- A level of assurance that critical decisions are not based on faulty information
- Accountability for safeguarding information

Roles and Responsibilities:-The following soft skills beneficial are:

- Reputation building
- Campus-wide coordination and communication
- Collaboration
- Campus-wide profiles

These soft skills are critical for effective engagement with diverse campus audiences.

- Senior leader of the institution
- Deans, Department Chairs and Directors
- IT managers

- Auditors
- Attorneys
- Human Resources
- Faculty
- Staff
- Students

Information Security Governance Structures:- Governance is highly dependent on the overall organization structure.

- Centralized maintain budget control and ensure implementation and monitoring of information security controls.
- Decentralized have policy and oversight responsibilities and budget responsibilities for their departmental security program not the operating unit information security program. Reporting structures are different as well.
- Governance structures can be hybrid, with a combination of characteristics from both centralized and decentralized.

Strategic Planning :-Strategic Plans, annual performance plans and annual program performance reports equal the recurring cycle of reporting, planning and execution. Each security plan must include:

- Mission, vision, goals, objectives and how they relate to the agency mission
- High-level plan for achieving information security goals and objectives including short- mid-term objective and performance targets and performance measures.

Risk Management:- Risk management is the ongoing process of identifying information security risks and implementing plans to address them. Often, the number of assets potentially at risk exceeds the resources available to manage them. It is therefore extremely important to know where to apply available resources to mitigate risk in an efficient and cost effective manner. Risk management is an activity directed towards assessment, mitigation, and monitoring of risks to an organization. Information security risk management is a major subset of the enterprise risk management process, which includes both the assessment of information security risks to the institution as well as the determination of appropriate management actions and established priorities for managing and implementing controls to protect against those risks. T his process can be broadly divided into two components:

1. **Risk assessment:-** Risk assessment identifies, quantifies, and prioritizes risks against both criteria for risk acceptance and objectives relevant to the organization. The assessment results guide the determination of appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The assessment should include both a systematic approach to estimating the magnitude of risks and a process for comparing estimated risks against risk criteria to determine the significance of the risks. The scope of a risk assessment can be either the whole organization, parts of the organization, an individual information system, or even specific system components or services.

2. **Risk treatment:-** A risk treatment decision needs to be made. Possible options for risk treatment include:

- Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance
- Applying appropriate controls to reduce the risks
- Avoiding risks by not allowing actions that would cause the risks to occur
- Transferring the associated risks to other parties, e.g. insurers or suppliers

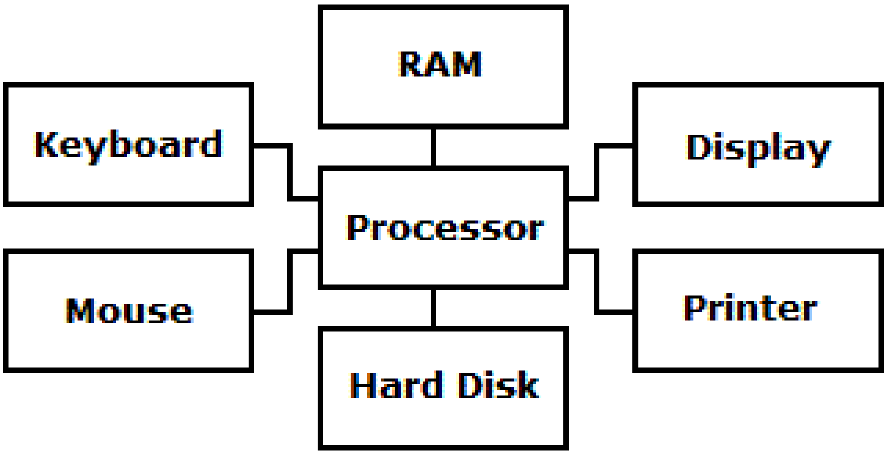
For each of the risks where the treatment decision is to apply some level of risk mitigation, appropriate controls may be selected from other sections of the Guide or elsewhere. Controls should be selected to ensure that risks are reduced to an acceptable level.

Security Architecture & Design Security Issues in Hardware:-

Security Architecture :-Security architects are the people responsible for a company’s computer system security. This could mean building new architecture that protects existing and future assets or identifying holes in current architecture that need updates. Security architecture required

- Acquire a complete understanding of a company’s technology and information systems
- Plan, research and design robust security architectures for any IT project
- Perform vulnerability testing, risk analyses and security assessments
- Research security standards, security systems and authentication protocols
- Develop requirements for local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), routers, firewalls, and related network devices
- Design public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures
- Prepare cost estimates and identify integration issues
- Review and approve installation of firewall, VPN, routers, IDS scanning technologies and servers
- Test final security structures to ensure they behave as expected
- Provide technical supervision for (and guidance to) a security team
- Define, implement and maintain corporate security policies and procedures
- Oversee security awareness programs and educational efforts
- Respond immediately to security-related incidents and provide a thorough post-event analysis
- Update and upgrade security systems as needed

Design Security Issues in Hardware:- With respect to chips and the devices in which they reside, tasks such as performing an Internet search, editing a document on a computer, making a mobile phone call, and conducting a financial transaction rely on a complex interplay between software and hardware. Once malicious hardware has been built into a chip, a hardware attack can be initiated and act in a wide variety of ways. An attack can be internally triggered, based, for example on the arrival of a particular calendar day. Alternatively, an external trigger could be hidden within data sent by an attacker. More complex hybrid triggers could also be used.



For example, a malicious circuit hidden within a GPS chip could be configured to attack only when the chip is located in a specific geographical area after a certain date.

Data Storage & Downloadable Devices:-

Data Storage:- Data storage is a general term for archiving data in electromagnetic or other forms for use by a computer or device. Different types of data storage play different roles in a computing environment. In addition to forms of hard data storage, there are now new options for remote data storage, such as cloud computing, that can revolutionize the ways that users access data.

Downloadable Devices:- Downloading is the transmission of a file from one computer system to another, usually smaller computer system. Example- Computer, Tab, Mobile etc.

Physical Security of IT Assets:- Physical security describes security measures that are designed to deny access to unauthorized personnel from physically accessing a building, facility, resource, or stored information. physical access controls for protected facilities are generally intended to:

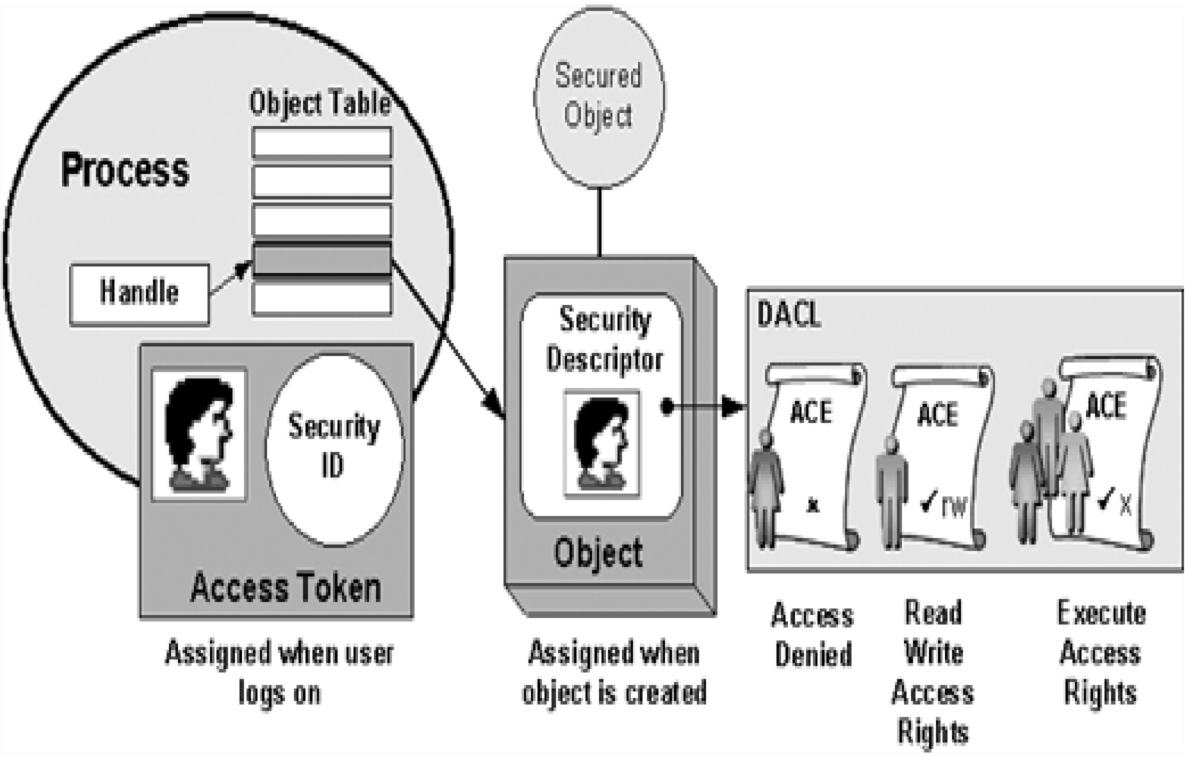
- deter potential intruders (e.g. warning signs and perimeter markings);
- distinguish authorized from unauthorized people (e.g. using keycards/access badges)
- delay, frustrate and ideally prevent intrusion attempts (e.g. strong walls, door locks and safes);
- detect intrusions and monitor/record intruders (e.g. intruder alarms and CCTV systems); and
- trigger appropriate incident responses (e.g. by security guards and police).

Access Control:- Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Normally, a user must first Login to a system, using some Authentication system. Access Control systems include-

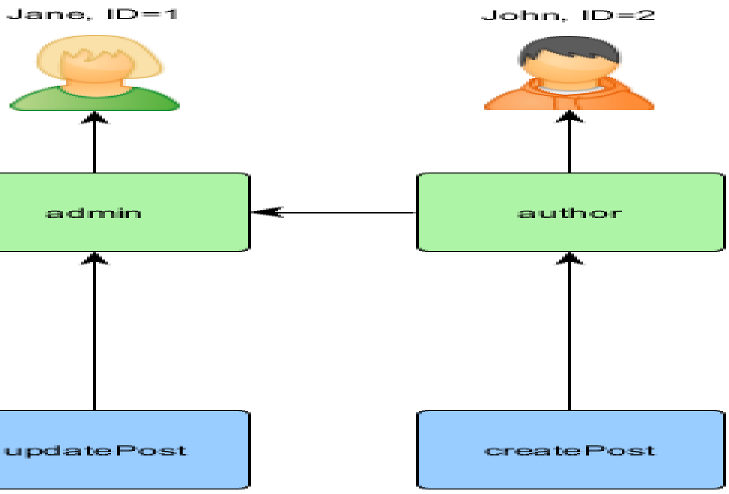
- File permissions, such as create, read, edit or delete on a file server.
- Program permissions, such as the right to execute a program on an application server.
- Data rights, such as the right to retrieve or update information in a database.

The four types of access control are:

- **Mandatory Access Control** :- Mandatory Access Control (MAC) is the strictest of all levels of control. MAC takes a hierarchical approach to controlling access to resources. Under a MAC enforced environment access to all resource objects (such as data files) is controlled by settings defined by the system administrator. Mandatory Access Control begins with security labels assigned to all resource objects on the system. These security labels contain two pieces of information a classification (top secret, confidential etc) and a category (which is essentially an indication of the management level, department or project to which the object is available). For example, cannot access a resource if they are not also a member of one of the required categories for that object.
- **Discretionary Access Control :-** Discretionary Access Control (DAC) allows each user to control access to their own data. For example, User A may provide read-only access on one of her files to User B, read and write access on the same file to User C full control.



- **Role Based Access Control:-** Role Based Access Control (RBAC) assigns permissions to particular roles in an organization. Users are then assigned to that particular role.



For example, an accountant in a company will be assigned to the Accountant role, gaining access to all the resources permitted for all accountants on the system. Similarly, a software engineer might be assigned to the developer role.

- **Rules Based Access Control :-** Rules Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator, When a particular account or group attempts to access a resource, the operating system checks the rules contained in the ACL for that object .Examples- permitting access for an account or group to a network connection at certain hours of the day or days of the week.

CCTV (Closed-Circuit Television) :- Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, casinos, airports, military installations, and

convenience stores. Video telephony is seldom called CCTV. Example when the environment is not suitable for humans. CCTV systems may operate continuously or only as required to monitor a particular event.

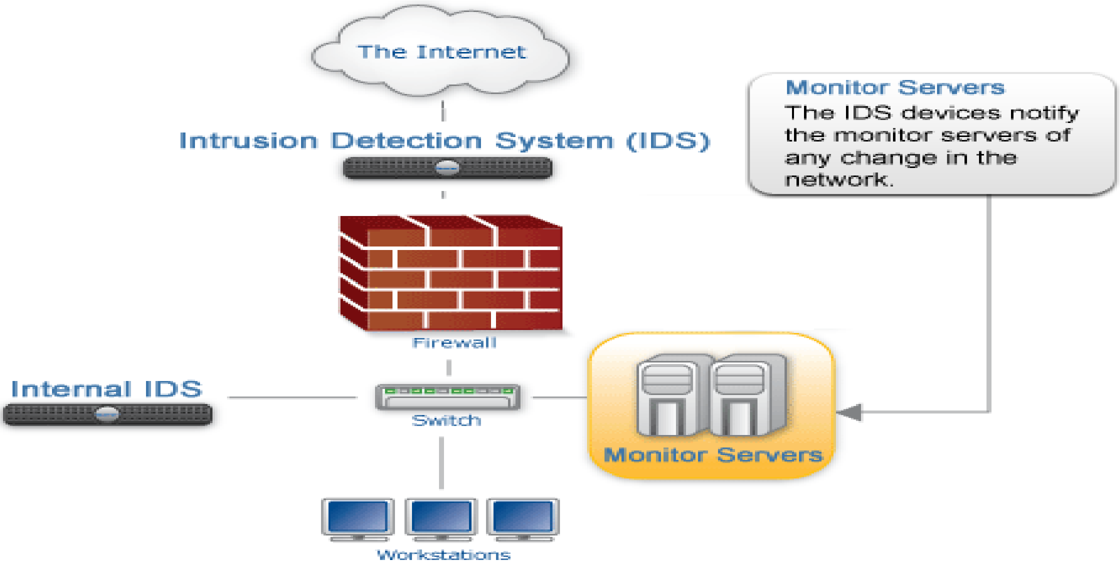
Application of CCTV:-

1. **Crime prevention:-** Surveillance systems were most effective in parking lots, where their use resulted in a 51% decrease in crime. Public transportation areas saw a 23% decrease in crimes**.** Systems in public settings were the least effective
2. **Industrial processes:-** Industrial processes that take place under conditions dangerous for humans are today often supervised by CCTV. These are mainly processes in the chemical

industry, the interior of reactors or facilities for manufacture of nuclear fuel. Special cameras for some of these purposes include line-scan cameras and thermo graphic cameras which allow operators to measure the temperature of the processes. The usage of CCTV in such processes is sometimes required by law.

3. **Traffic monitoring:-** Many cities and motorway networks have extensive traffic monitoring systems, using closed circuit television to detect congestion and notice accidents. Many of these cameras however, are owned by private companies and transmit data to drivers' GPS systems.
4. **Schools:-** CCTV may be installed in school to monitor visitors, track unacceptable student behavior and maintain a record of evidence in the event of a crime. There are some restrictions on installation, with cameras not being installed in an area where there is a "reasonable expectation of privacy". Cameras are generally acceptable in hallways, parking lots, front offices where students, employees, and parents come ,cafeterias, supply rooms and classrooms.

Intrusion Detection Systems:- An intrusion detection system (IDS) inspects all inbound (attacks from within the organization) and outbound (attacks from outside the organization) network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Intrusion detection functions include:

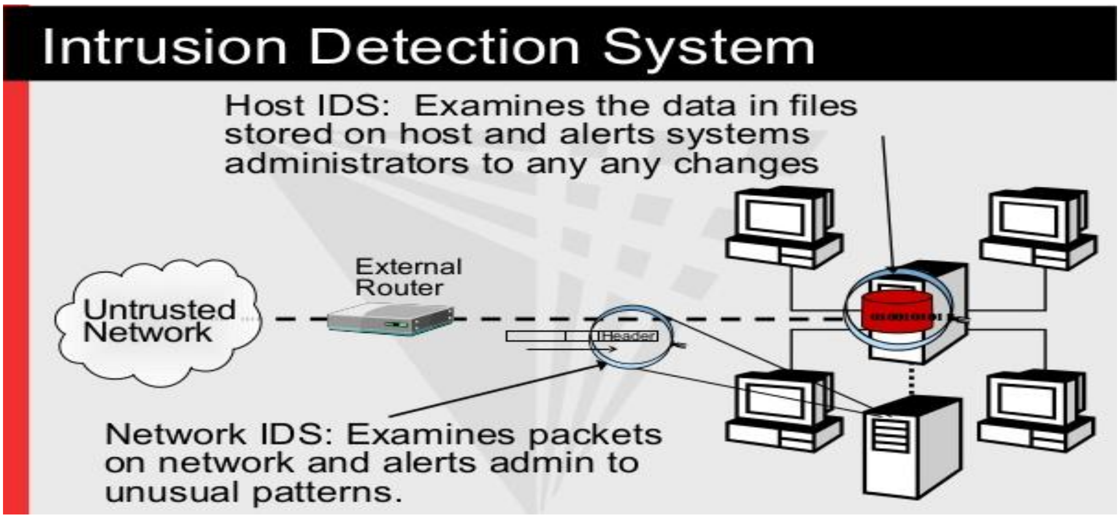


The IDS devices notify the monitor servers of any change in the network.

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

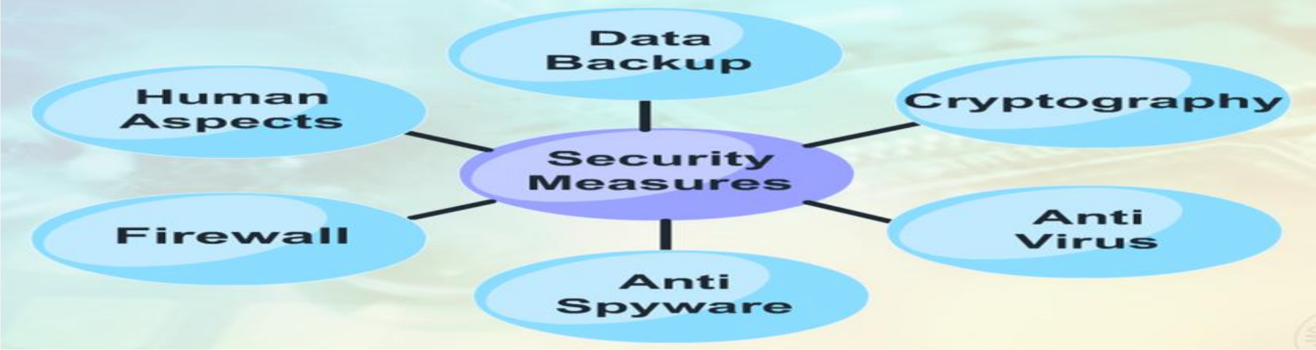
There are two ways to categorize an IDS:

- **Network-based: -** In a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by firewalls simplistic filtering rules. Catch threats targeting your vulnerable systems with signature-based anomaly detection and protocol analysis technologies. Identify the latest attacks, malware infections.


Intrusion Detection System
Host IDS: Examines the data in files stored on host and alerts systems administrators to any any changes
External Router
Untrusted Network
Header
Network IDS: Examines packets on network and alerts admin to unusual patterns.

- **Host-based:** - In a host-based system, the IDS examines at the activity on each individual computer or host. Analyze system behavior and configuration status to track user access and activity. Detect potential security exposures such as system compromise, modification of critical configuration files (e.g. registry settings, /etc/ passwd).

Backup Security Measures:- The average computer user should have at least three levels of security measures in place to protect their computer, Tablet and other electronic devices. Many unforeseen events can happen that result in data loss. Whether that data loss stems from file corruption, hardware failures, computer viruses, malware, hackers or natural disasters, it is just a matter of time before data loss will occur. Data loss is not the only risk of the lack of computer security. Viruses and other malicious applications can steal your personal information leading to identity theft. File backup is one of the most important aspects of protection from data loss.



Three Steps for a Solid Backup Scenario:-

- Backups should be performed locally to an external media like an external hard drive or DVD.
- Local backups need to be stored away from the computer, preferably to another location in case of fire or flooding.
- Online backups should be performed on a regular basis so important files can be accessed from other devices even if the backed up PC is no longer available.