INFORMATION SYSTEM SECURITY AND AUDIT
Chapter 1

SYSTEM CONCEPTS

Defining a system

System is a set of interacting or interdependent components forming an integrated whole or a set of elements (often called *'components')* and relationships which are different from relationships of the set or its elements to other elements or sets.

Therefore, a system is network of components work towards a single objective, if there is lack of co-ordination among components, it leads to counterproductive results. A system may have following features:

Data consists of the raw facts representing events occurring in the organization before they are organized into an understandable and useful form for humans.

Information is processed, organized and structured data. It provides context for data and enables decision making processes.
For example, a single customer's sale at a restaurant is data – this becomes information when the business is able to identify the most popular or least popular dish.structure".

An Information System (IS) can be any organized combination of people, hardware, software, communications networks, data resources, and policies and procedures that stores, retrieves, transforms, and disseminates information in an organization.

Therefore, an information system, can be defined as set of coordinated network of components which act together towards producing, distributing and or processing information.

An important factor of computer based information system is ***precision,*** *which may not apply to other types of systems.*

Components of information systems

The computer age introduced a new element to businesses, universities, and a multitude of other organizations: a set of components called the information system, which deals with collecting and organizing data and information. An information system is described as having five components.

Computer hardware

This is the physical technology that works with information. Hardware can be as small as a smartphone that fits in a pocket or as large as a supercomputer that fills a building. Hardware also includes the peripheral devices that work with computers, such as keyboards, external disk drives, and routers. With the rise of the Internet of things, in which anything from home appliances to cars to clothes will be able to receive and transmit data, sensors that interact with computers are permeating the human environment.

Computer software

The hardware needs to know what to do, and that is the role of software. Software can be divided into two types: system software and application software. The primary piece of system software is the operating system, such as Windows or iOS, which manages the hardware's operation. Application software is designed for specific tasks, such as handling a spreadsheet, creating a document, or designing a Web page.

Telecommunications

This component connects the hardware together to form a network. Connections can be through wires, such as Ethernet cables or fibre optics, or wireless, such as through Wi-Fi. A network can be designed to tie together computers in a specific area, such as an office or a school, through a local area network (LAN). If computers are more dispersed, the network is called a wide area network (WAN). The

Databases /Data

A database is a place where data is collected and from which it can be retrieved by querying it using one or more specific criteria. A data warehouse contains all of the data in whatever form that an organization needs.

Human resources and procedures

The final, and possibly most important, component of information systems is the human element: the people that are needed to run the system and the procedures they follow so that the knowledge in the huge databases and data warehouses can be turned into learning that can interpret what has happened in the past and guide future action.

Information Classification

After identifying the information to be protected, it is necessary to classify the information and organize it according to its sensitivity to loss, disclosure or unavailability.

The primary purpose of data classification is to indicate the protection level of confidentiality, Integrity and Availability required for each type of dataset.

Data classification helps to ensure that the data is protected in the most cost-effective manner.

Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed.

Data Classification Procedures

The following outlines the necessary steps for a proper classification program:

- Define classification levels.
- Specify the criteria that will determine how data is classified.
- Have the data owner indicate the classification of the data she is responsible for.
- Identify the data custodian who will be responsible for maintaining data and its security level.
- Indicate the security controls, or protection mechanisms, that are required for each classification level.
- Document any exceptions to the previous classification issues.
- Indicate the methods that can be used to transfer custody of the information to a different data owner.
- Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
- Indicate termination procedures for declassifying the data.
- Integrate these issues into the security-awareness program so that all employees understand how to handle data at different classification levels.

Classification Controls

The type of control implemented per classification depends upon the level of protection that management and the security team have determined is needed. Some of the controls are:

•Strict and granular access control for all levels of sensitive data and programs

•Encryption of data while stored and while in transmission

•Auditing and monitoring (determine what level of auditing is required and how long logs are to be retained)

•Separation of duties (determine whether two or more people need to be involved in accessing sensitive information to protect against fraudulent activities; if so, define and document procedures)

•Periodic reviews (review classification levels, and the data and programs that adhere to them, to ensure that they are still in alignment with business needs; data or applications may also need to be reclassified or declassified, depending upon the situation)

•Backup and recovery procedures (define and document)

•Change control procedures (define and document)

•File and file system access permissions (define and document)

Chapter Three

INFORMATION SECURITY

Is a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another.

Information Security management is a process of defining the security controls in order to protect the information assets.

Information security must be treated as a continuous effort to defend and protect a facility’s information assets.

Security controls are deployed with the intent of *deterring, delaying, detecting, or denying an attack.*

Information Security concepts

we will review the fundamental concepts of information systems security and discuss some of the measures that can be taken to mitigate security threats.

The three fundamental concepts of security are *availability, integrity, and confidentiality(*AIC)

Availability

Is the mirror image of confidentiality: while you need to make sure that your data can't be accessed by unauthorized users, you also need to ensure that it *can* be accessed by those who have the proper permissions. Access to information can be divided into several stages:

1. possibility for a subject to send a request for specific data to the information system (depends on the efficiency of the system interface, via which it receives such requests, and also on the serviceability and utilization of the communication channel between the subject and the server);

2. generation of a system response to a request over a time interval not exceeding the timeout (depends on the efficiency of the system, and also on its utilization processing other requests or other work);

3. possibility to deliver a response of the information system to the subject over a time interval not exceeding the timeout (depends on the efficiency of the system interface, via which it sends responses to requests, and also on the serviceability and utilization of the communication channel between the subject and the server).

Thus, availability of data or service on request depends on the efficiency and utilization of the communication channel between the user and the information system interface and on the efficiency and utilization of the information system itself.

The risk of malfunction of the information system comprising the information requested by the user depends on the reliability of sets of hardware and software components that comprise the system, and on the adequacy of the operator controlling their work. Availability violations arise bereason of non-compliance with standards in the system design, production or operation phase.

Integrity

Maintaining data in its correct state and preventing it from being improperly modified, either by accident or maliciously.

The risk of violating the integrity of information is provided by the following factors:

• Possibility of failure of hardware and software of the information system, as a violation of the relevance and consistency of the data can occur as a result of failures during their operation.

• Degree of reasonableness of algorithms and reliability of system authentication of users who have the right to edit the data stored in it.

• Possibility of having undocumented features in the software.

• Non-compliance with standards in the system design, production or operation phase.

• Imperfection of the organizational structure of the IS. For example, the need for frequent reconfiguration of the system or its parts may lead to violation of the confidentiality of stored and processed data in it, as well as additional costs.

• Human factor. For example, probability of social engineering in relation to persons who have access to editing the data stored in the system.

Integrity of data is protected when the assurance of accuracy and reliability of information and system is provided, and unauthorized modification is prevented.

Threat sources

- ✓ Viruses
- ✓ Logic Bombs
- ✓ Backdoors

Countermeasures

- ✓ Strict Access Control
- ✓ Intrusion Detection
- ✓ Hashing
- ✓ Availability

Availability ensures reliability and timely access to data and resources to authorized individuals.

Threat sources

- ✓ Device or software failure
- ✓ Environmental issues like heat, cold, humidity, static electricity, and contaminants can also affect system availability.
- ✓ Denial-of-service (DoS) attacks

Countermeasures

- ✓ Maintaining backups to replace the failed system
- ✓ IDS to monitor the network traffic and host system activities
- ✓ Use of certain firewall and router configurations

Confidentiality

Data is confidential when only those people who are authorized to access it can do so; to ensure confidentiality, you need to be able to identify who is trying to access data and block attempts by those without authorization.

By confidentiality we understand protection of information from unauthorized read access. The risk of violating the confidentiality of information is provided by the following factors:

• Degree of reasonableness of algorithms and reliability of system authentication of users who have the right to access the data stored in it.

• Possibility of having undocumented features in the software.

• Non-compliance with standards in the system design, production or operation phase.

• Imperfection of the organizational structure of the IS. For example, the need for frequent reconfiguration of the system or its parts may lead to violation of the confidentiality of stored and processed data in it, as well as additional costs.

• Human factor. For example, probability of social engineering in relation to persons who have access to the system. Insider threats

Ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of confidentiality should prevail while data resides on systems and devices within the network, as it is transmitted and once it reaches its destination.

Threat sources

- ✓ Network Monitoring
- ✓ Shoulder Surfing- monitoring key strokes or screen
- ✓ Stealing password files
- ✓ Social Engineering- one person posing as the actual

Countermeasures

- ✓ Encrypting data as it is stored and transmitted.
- ✓ By using network padding
- ✓ Implementing strict access control mechanisms and data classification
- ✓ Training personnel on proper procedures.

The Elements of Information Systems Security

All *risks, threats, and vulnerabilities* are measured for their potential capability to compromise one or all of the AIC principles

a) Vulnerability

It is a software, hardware, or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment.

Vulnerability characterizes the absence or weakness of a safeguard that could be exploited.

E.g.: a service running on a server, unpatched applications or operating system software, unrestricted modem dial-in access, an open port on a firewall, lack of physical security etc.

An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. These crimes target the confidentiality, integrity, or availability (known as the “CIA triad”) of resources possessed by an application, its creators, and its users.

b) Threat

Any potential danger to information or systems. A threat is a possibility that someone (person, s/w) would identify and exploit the vulnerability.

The entity that takes advantage of vulnerability is referred to as a threat agent. E.g.: A threat agent could be an intruder accessing the network through a port on the firewall

Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to significant financial losses. Information security damages can range from small losses to entire information system destruction. The effects of various threats vary considerably: some affect the confidentiality or integrity of **data** while others affect the **availability of a system.**

Currently, organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary means to combat them which continues to pose a challenge. To improve our understanding of security threats, we propose a security threat classification model which allows us to study the threats class impact instead of a threat impact as a threat varies over time.

c) Risk

Risk is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact. Reducing vulnerability and/or threat reduces the risk.

E.g.: If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.

Exposure

An exposure is an instance of being exposed to losses from a threat agent.

Vulnerability exposes an organization to possible damages.

E.g.:If password management is weak and password rules are not enforced, the company is exposed to the possibility of having users' passwords captured and used in an unauthorized manner.

Countermeasure or Safeguard

It is an application or a s/w configuration or h/w or a procedure that mitigates the risk.

E.g.: strong password management, a security guard, access control mechanisms within an operating system, the implementation of basic input/output system (BIOS) passwords, and security-awareness training.

The Relation between the Security Elements

Example 1

If a company has antivirus software but does not keep the virus signatures up-to-date, this is vulnerability. The company is vulnerable to virus attacks.

The threat is that a virus will show up in the environment and disrupt productivity.

The likelihood of a virus showing up in the environment and causing damage is the risk.

If a virus infiltrates the company's environment, then vulnerability has been exploited and the company is exposed to loss.

The countermeasures in this situation are to update the signatures and install the antivirus software on all computers

Threat Agent gives rise to Threat exploits Vulnerability leads to Risk can damage Assets and causes an Exposure can be counter measured by Safeguard directly effects Threat Agent

Example 2

Target: A bank contains money.

Threat: There are individuals who want, or need, additional money.

Vulnerability: The bank uses software that has a security flaw.

Exposure: 20% of the bank's assets are affected by this flaw.

Exploit: By running a small snippet of code (malware), the software can be accessed illegally.

Threat Agent: There are hackers who have learned how to use this malware to control the bank's software.

Exploitation: The hackers access the software using the malware and steal money.

Impact: The bank loses monetary assets, reputation, and future business.

Risk: The likelihood that a hacker will exploit the bank's software vulnerability and impact the bank's reputation and monetary resources.

Risk Management Practices

A risk management team should have the ability and follow the best practices, some of them which include:

- Establishing a risk acceptance level as provided by senior management
- Documenting risk assessment processes and procedures
- Establishing proper procedures for identifying and mitigating risks
- Getting support from senior management for appropriate resource and fund allocation
- Defining contingency plans where assessments indicate that they are necessary
- Ensure that security-awareness training is provided for all staff members associated with information assets.
- Strive to establish improvement (or risk mitigation) in specific areas when necessary
- Should map legal and regulation compliancy requirements to control and implement requirements
- Develop metrics and performance indicators to be able to measure and manage various types of risks
- Identify and assess new risks as the environment and company changes
- Integrate IRM and the organization's change control process to ensure that changes do not introduce new vulnerabilities

Ways to deal with Risk

There are four basic ways of dealing with risks:

- Transfer it: If a company's total or residual risk is too high and it purchases an insurance then it is transfer of risk to the insurance company
- Reject it: If a company is in denial about its risk or ignore it, it is rejecting the risk
- Reduce it: If a company implements countermeasures, it is reducing the risk
- Accept it: If a company understands the risk and decides not to implement any kind of countermeasures it is accepting the risk. And this is actually what all computer systems boil down to. There is no way to mitigate the risk if the system is going to connect to the internet. Having only one user without any networking with others computer systems is the closet you can ever get to not having any risks.

Risk Assessment/Analysis

Risk analysis is a method of identifying vulnerabilities and threat and assessing the possible damage to determine where to implement security safeguards

Why Risk Analysis?

- ✓ To ensure that security is cost effective, relevant, timely, and responsive to threat.
- ✓ To provide a cost/benefit comparison, this compares the annualized cost of safeguards to the potential cost of loss.
- ✓ Help integrate the security program objectives with the company's business objectives and requirements
- ✓ To provide an economic balance between the impact of the threat and the cost of the countermeasure.

Analyze the risk

Two approaches

- ✓ Quantitative Approach
- ✓ Qualitative Approach

A Quantitative Approach to Risk Analysis

Quantitative analysis uses risk calculations that attempt to predict the level of monetary losses and percentage of chance for each type of threat.

Quantitative risk analysis also provides concrete probability percentages when determining the likelihood of threats.

Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks.

Purely quantitative risk analysis is not possible, because the method attempts to quantify qualitative items, and there are always uncertainties in quantitative values

Sample Steps for a Quantitative Risk Analysis

Step 1: Assign Value to Assets- For each asset, answer the following questions to determine its value

- What is the value of this asset to the company?
- How much does it cost to maintain?
- How much does it make in profits for the company?
- How much would it be worth to the competition?
- How much would it cost to re-create or recover?
- How much did it cost to acquire or develop?
- How much liability are you under pertaining to the protection of this asset?

Step 2: Estimate Potential Loss per Threat- To estimate potential losses posed by threats, answer the following questions:

- What physical damage could the threat cause and how much would that cost?
- How much loss of productivity could the threat cause and how much would that cost?
- What is the value lost if confidential information is disclosed?
- What is the cost of recovering from this threat?
- What is the value lost if critical devices were to fail?
- What is the single loss expectancy (SLE) for each asset, and each threat?

Step 3: Perform a Threat Analysis- Take the following steps to perform a threat analysis

- Gather information about the likelihood of each threat taking place from people in each department, past records, and official security resources that provide this type of data.

- Calculate the annualized rate of occurrence (ARO), which is how many times the threat can take place in a 12-month period.

Step 4: Derive the Overall Loss Potential per Threat-To derive the overall loss potential per threat, do the following:

- Combine potential loss and probability.
- Calculate the annualized loss expectancy (ALE) per threat by using the information calculated in the first three steps.
- Choose remedial measures to counteract each threat.
- Carry out cost/benefit analysis on the identified countermeasures.

Step 5: Reduce, Transfer, or Accept the Risk- For each risk, you can choose whether to reduce, transfer, or accept the risk:

Risk reduction methods

- o Install security controls and components.
- o Improve procedures.
- o Alter environment.
- o Provide early detection methods to catch the threat as it's happening and reduce the possible damage it can cause.
- o Produce a contingency plan of how business can continue if a specific threat takes place, reducing further damages of the threat.
- o Erect barriers to the threat.
- o Carry out security-awareness training.

Risk transfer- Buy insurance to transfer some of the risk, for example.

Risk acceptance- Live with the risks and spend no more money toward protection.

Quantitative Risk Analysis Metrics

- Single loss expectancy (SLE) - The amount of loss due to a single occurrence of a threat.
- Annualized loss expectancy (ALE) - The estimated loss per annum.
- Exposure factor (EF) - Represents the percentage of loss a realized threat could have on a certain asset.
- Annualized rate of occurrence (ARO) – It is the value that represents the estimated frequency of a specific threat taking place within a one-year timeframe. It can range from 0.0 to 1.0.

Results of a Quantitative Risk Analysis

The following is a short list of what generally is expected from the results of a risk analysis

- Monetary values assigned to assets
- Comprehensive list of all possible and significant threats
- Probability of the occurrence rate of each threat
- Loss potential the company can endure per threat in a 12-month time span
- Recommended safeguards, countermeasures, and actions analysis.

Quantitative Pros

- Requires more complex calculations
- Is easier to automate and evaluate
- Used in risk management performance tracking
- Provides credible cost/benefit analysis
- Shows clear-cut losses that can be accrued within one year's time

Quantitative Cons

- Calculations are more complex. Can management understand how these values were derived?
- Without automated tools, this process is extremely laborious.
- Big need to gather detailed information about environment.
- Standards are not available. Each vendor has its own way of interpreting the processes and their results.

A Qualitative Approach to Risk Analysis

- In Qualitative approach, we walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures.
- The Qualitative analysis techniques include judgment, best practices, intuition, and experience.
- Qualitative Risk Analysis Techniques
- Delphi -A group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result to a particular threat will be. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.

  Brainstorming, Focus groups, Surveys, Questionnaires, Checklists, One-on-One meetings and Interviews.

The risk analysis team will determine the best technique for the threats that need to be assessed and the culture of the company and individuals involved with the analysis.

The team that is performing the risk analysis gathers personnel who have experience and education on the threats being evaluated. When this group is presented with a scenario that describes threats and loss potential, each member responds with their gut feeling and experience on the likelihood of the threat and the extent of damage that may result.

Qualitative Pros

- ✓ Requires simple calculations
- ✓ Involves high degree of guesswork
- ✓ Provides general areas and indications of risk
- ✓ Provides the opinions of the individuals who know the processes best

Qualitative Cons

- ✓ The assessments and results are basically subjective.
- ✓ Usually eliminates the opportunity to create a dollar value for cost/benefit discussions.
- ✓ Difficult to track risk management objectives with subjective measures.
- ✓ Standards are not available. Each vendor has its own way of interpreting the processes and their results.

Chapter Four

INFORMATION SECURITY CONTROLS

Introduction

Information security controls are measures taken to reduce information security risks such as information systems breaches, data theft, and unauthorized changes to digital information or systems. These security controls are intended to help protect the availability, confidentiality, and integrity of data and networks, and are typically implemented after an information security risk assessment.

The first action of a management program to implement information security is to have a security program in place.

Approaches to build a security program

- Top-Down Approach

The initiation, support, and direction comes from the top management and work their way through middle management and then to staff members.

Treated as the best approach but seems to base on the I get paid more therefor I must know more about everything type of mentality.

Ensures that the senior management who are ultimately responsible for protecting the company assets is driving the program.

- Bottom-Up Approach

The lower-end team comes up with a security control or a program without proper management support and direction.

Security Controls can be classified into three categories:

- ✓ Administrative Controls
- ✓ Technical control
- ✓ Physical controls

Administrative Controls which include

- Developing and publishing of policies, procedures, standards and guidelines.
- Screening of personnel.
- Conducting security-awareness training and
- Implementing change control procedures.

Policy and Procedures

- A security policy is a high-level plan that states management’s intent pertaining to how security should be practiced within an organization, what actions are acceptable, and what level of risk the company is willing to accept. This policy is derived from the laws, regulations, and business objectives that shape and restrict the company.
- The security policy provides direction for each employee and department regarding how security should be implemented and followed, and the repercussions for noncompliance. Procedures, guidelines, and standards provide the details that support and enforce the company’s security policy.

Personnel Controls

- Personnel controls indicate how employees are expected to interact with security mechanisms, and address noncompliance issues pertaining to these expectations.
- Change of Status: These controls indicate what security actions should be taken when an employee is hired, terminated, suspended, moved into another department, or promoted.
- Separation of duties: The separation of duties should be enforced so that no one individual can carry out a critical task alone that could prove to be detrimental to the company.

Example: A bank teller who has to get supervisory approval to cash checks over $2000 is an example of separation of duties. For a security breach to occur, it would require collusion, which means that more than one person would need to commit fraud, and their efforts would need to be concerted. The use of separation of duties drastically reduces the probability of security breaches and fraud.

- Rotation of duties means that people rotate jobs so that they know how to fulfill the obligations of more than one position. Another benefit of rotation of duties is that if an individual attempts to commit fraud within his position, detection is more likely to happen if there is another employee who knows what tasks should be performed in that position and how they should be performed.

Security-Awareness Training

- This control helps users/employees understand hot to properly access resources, why access controls are in place and the ramification for not using the access controls properly.

Supervisory Structure

Management must construct a supervisory structure which enforces management members to be responsible for employees and take a vested interest in their activities. If an employee is caught hacking into a server that holds customer credit card information, that employee and her supervisor will face the consequences?

Job Rotation

Job Rotation is an approach to management development where an individual is moved through a schedule of assignments designed to give him or her a breath of exposure to the entire operation.

Job rotation is also practiced to allow qualified employees to gain more insights into the processes of a company and to increase job satisfaction through job variation.
Separation of Duties

Separation of duties (SoD)
Is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties or, in the political realm, separation of powers.

SoD in basic terms that is no single individuals should have controls over two or more phases of a transaction or operation, so that a deliberate fraud is more difficult to occur because it requires collusion of two or more individuals or parties.

With the concept of SoD, business critical duties can be categorized into four types of functions, authorization, custody, record keeping and reconciliation. In a perfect system, no one person should handle more than one type of function.

In information systems, segregation of duties helps reduce the potential damage from the actions of one person. IS or end-user department should be organized in a way to achieve adequate separation of duties

Control Mechanisms to enforce SoD

There are several control mechanisms that can help to enforce the segregation of duties:

Audit trails enable IT managers or Auditors to recreate the actual transaction flow from the point of origination to its existence on an updated file. Good audit trails should be enabled to provide information on who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated.

Reconciliation of applications and an independent verification process is ultimately the responsibility of users, which can be used to increase the level of confidence that an application ran successfully.

Exception reports are handled at supervisory level, backed up by evidence noting that exceptions are handled properly and in timely fashion. A signature of the person who prepares the report is normally required.

Manual or automated system or application transaction logs should be maintained, which record all processed system commands or application transactions.

Supervisory review should be performed through observation and inquiry and the trust built with directory one-level up managers.

To compensate repeated mistakes or intentional failures by following a prescribed procedure, independent reviews are recommended. Such reviews can help detect errors and irregularities but are usually expensive can raise questions as to how much can an outside independent review once a quarter know about your processes compared to people within and what level of trust can be built with those independent reviewers.

Least Privilege

The principle of least privilege, also known as the principle of minimal privilege or just least privilege, requires that in a particular abstraction layer of a computing environment every module (such as a process, a user or a program on the basis of the layer we are considering) must be able to access only such information and resources that are necessary to its legitimate purpose.
Note: This principle is a useful security tool, but it has never been successful at enforcing high assurance security on a system.

Benefits

Better system stability. When code is limited in the scope of changes it can make to a system, it is easier to test its possible actions and interactions with other applications. In practice for example, applications running with restricted rights will not have access to perform operations that could crash a machine, or adversely affect other applications running on the same system.

Better system security. When code is limited in the system-wide actions it may perform, vulnerabilities in one application cannot be used to exploit the rest of the machine. For example, Microsoft states "Running in standard user mode gives customers increased protection against inadvertent system-level damage caused by "shatter attacks" and malware, such as root kits, spyware, and undetectable viruses." [1]

Ease of deployment. In general, the fewer privileges an application requires the easier it is to deploy within a larger environment. This usually results from the first two benefits, applications that install device drivers or require elevated security privileges typically have addition steps involved in their deployment, for example on Windows a solution with no device drivers can be run directly with no installation, while device drivers must be installed separately using the Windows installer service in order to grant the driver elevated privileges

Testing

- This control states that all security controls, mechanisms, and procedures are tested on a periodic basis to ensure that they properly support the security policy, goals, and objectives set for them.
- The testing can be a drill to test reactions to a physical attack or disruption of the network, a penetration test of the firewalls and perimeter network to uncover vulnerabilities, a query to employees to gauge their knowledge, or a review of the procedures and standards to make sure they still align with business or technology changes that have been implemented.

Examples of Administrative Controls

- Security policy
- Monitoring and supervising
- Separation of duties
- Job rotation
- Information classification
- Personnel procedures
- Investigations
- Testing
- Security-awareness and training

TECHNICAL CONTROLS

Technical or Logical Controls which include

- Implementing and maintaining access control mechanisms.
- Password and resource management.
- Identification and authentication methods
- Security devices and
- Configuration of the infrastructure.
- Implementing and maintaining access control mechanisms.

Implementing and maintaining access control mechanisms

Access controls are security features that control how users and systems communicate and interact with other systems and resources.

Access is the flow of information between a subject and an object.

A *subject* is an active entity that requests access to an object or the data within an object. E.g.: user, program, process etc.

An *object* is a passive entity that contains the information. E.g.: Computer, Database, File, Program etc.

Access Control Challenges

- Various types of users need different levels of access - Internal users, contractors, outsiders, partners, etc.
- Resources have different classification levels- Confidential, internal use only, private, public, etc.
- Diverse identity data must be kept on different types of users - Credentials, personal data, contact information, work-related data, digital certificates, cognitive passwords, etc.
- The corporate environment is continually changing- Business environment needs, resource access needs, employee roles, actual employees, etc.

Access Control Principles

- Principle of Least Privilege: States that if nothing has been specifically configured for an individual or the groups, he/she belongs to, the user should not be able to access that resource i.e.Default no access
- Separation of Duties

- Need to know : It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties

Identification, Authentication and Authorization

Identification describes a method of ensuring that a subject is the entity it claims to be. E.g.: A user name or an account no.

Authentication is the method of proving the subjects identity. E.g.: Password, Passphrase, PIN

Authorization is the method of controlling the access of objects by the subject. E.g.: A user cannot delete a particular file after logging into the system

Note: There must be a three step process of Identification, Authentication and Authorization in order for a subject to access an object

Identification

When issuing identification values to users or subjects, ensure that

- Each value should be unique, for user accountability
- A standard naming scheme should be followed
- The values should be non-descriptive of the users position or task
- The values should not be shared between the users.

Authentication Factors

There are 3 general factors for authenticating a subject.

- Something a person knows- E.g.: passwords, PIN- least expensive, least secure
- Something a person has – E.g.: Access Card, key- expensive, secure
- Something a person is- E.g.: Biometrics- most expensive, most secure

Note: For a strong authentication to be in process, it must include two out of the three authentication factors- also referred to as two factor authentication.

Authentication Methods

Biometrics

- Verifies an individuals identity by analyzing a unique personal attribute or behavior
- It is the most effective and accurate method for verifying identification.
- It is the most expensive authentication mechanism
- Types of Biometric Systems
    - *Finger Print*- are based on the ridge endings, bifurcation exhibited by the friction edges and some minutiae of the finger
    - *Palm Scan*- are based on the creases, ridges, and grooves that are unique in each individuals palm
    - Hand Geometry- are based on the shape (length, width) of a persons hand and fingers
    - *Retina Scan*- is based on the blood vessel pattern of the retina on the backside of the eyeball.
    - *Iris Scan*- is based on the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas and furrows.
    - *Signature Dynamics*- is based on electrical signals generated due to physical motion of the hand during signing a document
    - *Keyboard Dynamics*- is based on electrical signals generated while the user types in the keys (passphrase) on the keyboard.
    - *Voice Print*- based on human voice
    - *Facial Scan*- based on the different bone structures, nose ridges, eye widths, forehead sizes and chin shapes of the face.
    - *Handy Topography*- based on the different peaks, valleys, overall shape and curvature of the hand.

Passwords

- It is the most form of system identification and authentication mechanism
- A password is a protected string of characters that is used to authenticate an individual
- Password Management
    - Password should be properly guaranteed, updated, and kept secret to provide and effective security
    - Passwords generators can be used to generate passwords that are uncomplicated, pronounceable, non-dictionary words.
    - If the user chooses his passwords, the system should enforce certain password requirement like insisting to use special char, no of char, case sensitivity etc.)

Access Control Threats

Denial of Service(DoS/DdoS)

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

The purpose of DoS attacks is to force the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service

Types of DoS Attacks

A DoS attack can be perpetrated in a number of ways. There are five basic types of attack:

- Consumption of computational resources, such as bandwidth, disk space, or CPU time;
- Disruption of configuration information, such as routing information;
- Disruption of state information, such as unsolicited resetting of TCP sessions;
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Countermeasures

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software.
- Install a firewall, and configure it to restrict traffic coming into and leaving your computer.
- Follow good security practices for distributing your email address.Applying email filters may help you manage unwanted traffic.

Buffer Overflows

A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

Buffer Overflow Techniques

- *Stack Buffer Overflow*
  - A stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside of the intended data structure; usually a fixed length buffer.

  - Stack buffer overflow bugs are caused when a program writes more data to a buffer located on the stack than there was actually allocated for that buffer. This almost always results in corruption of adjacent data on the stack, and in cases where the overflow was triggered by mistake, will often cause the program to crash or operate incorrectly.

  - A technically inclined and malicious user may exploit stack-based buffer overflows to manipulate the program in one of several ways:

    - By overwriting a local variable that is near the buffer in memory on the stack to change the behaviour of the program which may benefit the attacker.

    - By overwriting the return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input filled buffer.

    - By overwriting a function pointer,or exception handler, which is subsequently executed.

- *Heap Buffer Overflow*

  - A heap overflow is another type of buffer overflow that occurs in the heap data area. Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.

  - Exploitation goes as follows: If an application copies data without first checking to see if it fits into the chunk (blocks of data in the heap), the attacker could supply the application with a piece of data that is too large, overwriting heap management information (metadata) of the next chunk. This allows an attacker to overwrite an arbitrary memory location with four bytes of data. In most environments, this may allow the attacker control over the program execution.

Countermeasure

- Choice of programming language
- Use of safe libraries

- Stack-smashing protection which refers to various techniques for detecting buffer overflows on stack-allocated variables.The most common implementation being StackGuard, and SSP

- Executable space protection which is the marking of memory regions as non-executable, such that an attempt to execute machine code in these regions will cause an exception. It makes use of hardware features such as the NX bit (Non Execute bit).

- Address space layout randomization: A technique which involves arranging the positions of key data areas, usually including the base of the executable and position of libraries, heap, and stack, randomly in a process' address space.

- Deep packet inspection:It is a form of computer network packet filtering that examines the data and/or header part of a packet as it passes an inspection point, searching for non-protocol compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information. It also called Content Inspection or Content Processing.

Spoofing/Masquerading

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Popular Spoofing Techniques

- *Man-in-the-middle attack (MITM):*An attack in which an attacker is able to read, insert and modify at will messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims
- *IP address Spoofing* : refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
- *URL spoofing*: A Spoofed URL describes one website that poses as another
- *Phishing* :An attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.
- *Referrer spoofing*:It is the sending of incorrect referrer information along with an HTTP request, sometimes with the aim of gaining unauthorized access to a web site. It can also be used because of privacy concerns, as an alternative to sending no referrer at all.
- *Spoofing of file-sharing Networks*: Polluting the file-sharing networks where record labels share files that are mislabeled, distorted or empty to discourage downloading from these sources.
- *Caller ID spoofing* :This allows callers to lie about their identity, and present false names and numbers, which could of course be used as a tool to defraud or harass
- *E-mail address spoofing:*A technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message by changing certain properties of the e-mail, such as the From, Return-Path and Reply-To fields.
- *Login spoofing* : A technique used to obtain a user's password. The user is presented with an ordinary looking login prompt for username and password, which is actually a malicious program, usually called a Trojan horse under the control of the attacker. When the username and password are entered, this information is logged or in some way passed along to the attacker, breaching security.

Countermeasures

- Be skeptical of e-mails indicating that you need to make changes to your accounts or warnings indicating that accounts will be terminated without you doing some type of activity online.
- Call the legitimate company to find out if this is a fraudulent message.
- Review the address bar to see if the domain name is correct.
- When submitting any type of financial information or credential data, an SSL connection should be set up, which is indicated in the address bar (https://) and a closed-padlock icon in the browser at the bottom-right corner.

Emanations

All electronic devices emit electrical signals. These signals can hold important information, and if an attacker buys the right equipment and positions himself in the right place, he could capture this information from the airwaves and access data transmissions as if he had a tap directly on the network wire.

Countermeasure

- Tempest: Tempest is the name of a program, and now a standardized technology that suppresses signal emanations with shielding material. Vendors who manufacture this type of equipment must be certified to this standard. In devices that are Tempest rated, other components are also modified, especially the power supply, to help reduce the amount of electricity that is used unlike the normal devices which have just an outer metal coating, referred to as a Faraday cage. This type of protection is usually needed only in military institutions, although other highly secured environments do utilize this type of safeguard.

Shoulder Surfing

Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is particularly effective in crowded places because it's relatively easy to observe someone as they:

  - Fill out a form
  - Enter their PIN at an automated teller machine or a POS Terminal
  - Use a calling card at a public pay phone
  - Enter passwords at a cybercafe, public and university libraries, or airport kiosks.
  - Enter a digit code for a rented locker in a public place such as a swimming pool or airport.

- Shoulder surfing is also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand.

- Recent automated teller machines now have a sophisticated display which discourages shoulder surfers. It grows darker beyond a certain viewing angle, and the only way to tell what is displayed on the screen is to stand directly in front of it.

Object Reuse

Object reuse issues pertain to reassigning to a subject media that previously contained one or more objects.
The sensitive information that may be left by a process should be securely cleared before allowing another process the opportunity to access the object. This ensures that information not intended for this individual or any other subject is not disclosed.
For media that holds confidential information, more extreme methods should be taken to ensure that the files are actually gone, not just their pointers.

Countermeasures

- Sensitive data should be classified by the data owners.
- How the data is stored and accessed should also be strictly controlled and audited by software controls.
- Before allowing one subject to use media that was previously used, the media should be erased or degaussed. If media holds sensitive information and cannot be purged, there should be steps on how to properly destroy it so that there is no way for others to obtain this information.

Data Remanence

Data remanence is the residual representation of data that has been in some way been nominally erased or removed. This residue may be due to data being left intact by a nominal delete operation, or through physical properties of the storage medium.
Data remanence may make inadvertent disclosure of sensitive information possible, should the storage media be released into an uncontrolled environment.

Countermeasures

- Methods to Countermeasure
  - Overwriting
    - A common method used to counter data remanence is to overwrite the storage medium with new data. This is often called a wiping or shredding a file or disk. Because such methods can often be implemented in software alone, and may be able to selectively target only part of a medium, it is a popular, low-cost option for some applications.
    - The simplest overwrite technique writes the same data everywhere -- often just a pattern of all zeros. At a minimum, this will prevent the data from being retrieved simply by reading from the medium again, and thus is often used for clearing.
  - Degaussing
    - Degaussing is the removal or reduction of a magnetic field. Applied to magnetic media, degaussing may purge an entire media element quickly and effectively. A device, called a degausser, designed for the media being erased, is used.

    - Degaussing often renders hard disks inoperable, as it erases low-level formatting which is only done at the factory, during manufacture. Degaussed floppy disks can generally be reformatted and reused.

- Encryption

    - Encrypting data before it is stored on the medium may mitigate concerns about data remanence. If the decryption key is strong and carefully controlled (i.e., not itself subject to data remanence), it may effectively make any data on the medium unrecoverable. Even if the key is stored on the medium, it may prove easier or quicker to overwrite just the key, vs the entire disk.

    - Encryption may be done on a file-by-file basis, or on the whole disk.

- Physical destruction

    - Physical destruction of the data storage medium is generally considered the most certain way to counter data remanence, although also at the highest cost. Not only is the process generally time-consuming and cumbersome, it obviously renders the media unusable. Further, with the high recording densities of modern media, even a small media fragment may contain large amounts of data.

    - Specific destruction techniques include:

        - Physically breaking the media apart, by grinding, shredding, etc.

        - Incinerating

        - Phase transition (i.e., liquification or vaporization of a solid disk)

        - Application of corrosive chemicals, such as acids, to recording surfaces

        - For magnetic media, raising its temperature above the Curie point

Backdoor/Trapdoor

A backdoor is a malicious computer program or particular means that provide the attacker with unauthorized remote access to a compromised system exploiting vulnerabilities of installed software and bypassing normal authentication.

A backdoor works in background and hides from the user. It is very similar to a virus and therefore is quite difficult to detect and completely disable.

A backdoor is one of the most dangerous parasite types, as it allows a malicious person to perform any possible actions on a compromised computer. The attacker can use a backdoor to

- spy on a user,
- manage files,

- install additional software or dangerous threats,

- control the entire system including any present applications or hardware devices,
- shutdown or reboot a computer or
- attack other hosts.

Often a backdoor has additional harmful capabilities like keystroke logging, screenshot capture, file infection, even total system destruction or other payload. Such parasite is a combination of different privacy and security threats, which works on its own and doesn’t require to be controlled at all.

Countermeasure

- Powerful antivirus and anti-spyware products

Dictionary Attacks

Dictionary attacks are launched by programs which are fed with a lists (dictionaries) of commonly used words or combinations of characters, and then compares these values to capture passwords.

Once the right combination of characters is identified, the attacker can use this password to authenticate herself as a legitimate user.

Sometimes the attacker can even capture the password file using this kind of activity.

Countermeasures

To properly protect an environment against dictionary and other password attacks, the following practices should be followed:

- Do not allow passwords to be sent in cleartext.
- Encrypt the passwords with encryption algorithms or hashing functions.
- Employ one-time password tokens.
- Use hard-to-guess passwords.
- Rotate passwords frequently.
- Employ an IDS to detect suspicious behavior.
- Use dictionary cracking tools to find weak passwords chosen by users.
- Use special characters, numbers, and upper- and lowercase letters within the password.
- Protect password files.

Bruteforce Attacks

- Brute force is defined as “trying every possible combination until the correct one is identified.”

- The most effective way to uncover passwords is through a hybrid attack, which combines a dictionary attack and a brute force attack
- A brute force attack is also known as an exhaustive attack.
- These are usually used for wardialing in hopes of finding a modem that can be exploited to gain unauthorized access.

Countermeasures

For phone brute force attacks, auditing and monitoring of this type of activity should be in place to uncover patterns that could indicate a wardialing attack:

- Perform brute force attacks to find weaknesses and hanging modems.
- Make sure only necessary phone numbers are made public.
- Provide stringent access control methods that would make brute force attacks less successful.
- Monitor and audit for such activity.
- Employ an IDS to watch for suspicious activity.
- Set lockout thresholds.

Social Engineering

Social engineering is a collection of techniques used for manipulation of the natural human tendency to trust in order to obtain information that will allow a hacker to gain unauthorized access to a valued system and the information that resides on that system.

Forms of a Social engineering attack

- Physical: the workplace, the phone, your trash, and even on-line
- Psychological: Persuasion
- Reverse Social Engineering

Countermeasures

- Having proper security policies in place which addresses both physical and psychological aspects of the attack
- Providing proper training to employees, helpdesk personnel

Access Control Technologies

Single Sign-On

- SSO is a technology that allows a user to enter credentials one time and be able to access all resources in primary and secondary network domains

Advantages

- Reduces the amount of time users spend authenticating to resources.
- Enable the administrator to streamline user accounts and better control access rights
- Improves security by reducing the probability that users will write down their passwords
- Reduces the administrators time in managing the access permissions

Kerberos

- Kerberos is an authentication protocol that was designed in mid-1980 as part of MIT's project Athena.
- It works in a C/S model and is based on symmetric key cryptography
- It is widely used in UNIX systems and also the default authentication method for windows 2k and 2k3 and is the de-facto standard for heterogeneous networks.

Kerberos Components

- Key Distribution Center (KDC)
  - Holds all users and services secret key and info about the principles in the database
  - Provides an authentication service with the help of a service called AS
  - Provides key distribution functionality
  - Provides a ticket granting service (TGS)
- Secret Keys are the keys shared between principle and KDC generally using symmetric key cryptography algorithm that are used to authenticate the principles and communicate securely
- Principles are users, applications or any network services
- A ticket is a token generated by KDC and given to a principle when one principle need to authenticate another principle
- Realm is a set of principles. A KDC can be responsible for one or more realms. Realms allow an administrator to logically group resources and users.
- Session Keys are the keys shared between the principles that will enable them communicate security

SESAME

- SESAME (Secure European Systems for Applications in a Multi-vendor Environment) is a SSO technology that was developed to extend Kerberos functionality and improve upon its weakness.
- SESAME uses a symmetric and asymmetric cryptographic technique to protect exchanges of data and to authenticate subjects to network resources.
- SESAME uses digitally signed privileged Attribute Certificates (PAC) to authenticate subjects to objects. PAC contains the subject's identity, access capabilities for the object, access time period, and life time of the PAC

Security Domain

- A domain is a set of resources that are available to a subject.
- A security domain refers to the set the resources working under the same security policy and managed by the same group.
- Domains can be separated by logical boundaries, such as
    - Firewalls with ACL's
    - Directory services making access decisions
    - Objects that have their own ACL's indicating which individual or group can access them.
- Domains can be architected in a hierarchical manner that dictates the relationship between the different domains and the ways in which subjects within the different domains can communicate.
- Subjects can access resources in domains of equal or lower trust levels.

Thin Clients

- Thin clients are diskless computers that are sometimes called as dumb terminals.
- It is based on C/S technology where a user is supposed to logon to a remote server to use the computing and network resources.
- When the user starts the client, it runs a short list of instructions and then points itself to a server that will actually download the operating system, or interactive operating software, to the terminal. This enforces a strict type of access control, because the computer cannot do anything on its own until it authenticates to a centralized server, and then the server gives the computer its operating system, profile, and functionality.
- Thin-client technology provides another type of SSO access for users, because users authenticate only to the central server or mainframe, which then provides them access to all authorized and necessary resources.

Access Control Models

- An access control model is a framework that dictates how subjects access objects.
- It uses access control technologies and security mechanisms to enforce the rules and objectives of the model.
- There are three main types of access control models:
  - Discretionary,
  - Mandatory, and
  - Nondiscretionary (also called role-based).

Discretionary Access Control

- The control of access is based on the discretion (wish) of the owner
- A system that uses DAC enables the owner of the resource to specify which subjects can access specific resources
- The most common implementation of DAC is through ACL's which are dictated and set by the owners and enforced by the OS.
- Examples: Unix, Linux, Windows access control is based on DAC
- DAC systems grant or deny access based on the identity of the subject. The identity can be user identity or a group identity (Identity based access control)

Mandatory Access Control

- This model is very structured and strict and is based on a security label (also known as sensitivity label) attached to all objects
- The subjects are given security clearance by classifying the subjects as secret, top secret, confidential etc.) and the objects are also classified similarly
- The clearance and the classification data is stored in the security labels, which are bound to the specific subject and object.
- When the system makes a decision about fulfilling a request to access an object it is based on the clearance of the subject. The classification of the object and the security policy of the system
- This model is used and is suitable for military systems where classifications and confidentiality is of at most important
- SE Linux, by NSA, trusted Solaris are examples of this model
- Security label are made up of a classification and categories, where classification indicates the security level and the categories enforce need to know rules.

Non Discretionary or Role Based Access Control

- A RBAC is based on user roles and uses a centrally administered set of controls to determine how subjects and objects interact.
- The RBAC approach simplifies the access control administration
- It is a best system for a company that has high employee turnover.
- Note: The RBAC can be generally used in combination with MAC and DAC systems

Access Control Administration

Access control administration can be done in two ways.

- Centralized
- Decentralized.

Centralized Access Control

- Here one entity (dept or an individual) is responsible for overseeing access to all corporate resources.
- This type of administration provides a consistent and uniform method of controlling users access rights.
- Example: RADIUS, TACACS and Diameter

Decentralized Access Control

- A decentralized access control administration method gives control of access to the people closer to the resources
- In this approach, it is often the functional manager who assigns access control rights to employees.
- Changes can happen faster through this type of administration because not just one entity is making changes for the whole organization.
- There is a possibility for conflicts to arise that may not benefit the organization as because different managers and departments can practice security and access control in different ways.
- There is a possibility of certain controls to overlap, in which case actions may not be properly proscribed or restricted.
- This type of administration does not provide methods for consistent control, as a centralized method would.

Access Control Monitoring

Access Control Monitoring is a method of keeping track of who attempts to access specific network resources

The ACM system can fall into two categories: Intrusion Prevention System (IPS) and Intrusion Detection System (IDS)

Intrusion Detection Systems

Basic Concepts

Intrusion detection is the process of detecting an unauthorized use of, or attack upon, a computer, network, or a telecommunication infrastructure.
IDS are designed to aid in mitigating the damage that can be caused by hacking, or breaking into sensitive computer and network systems.

Common Functions of an IDS

- Watch for attacks
- Parse audit logs
- Protect system files
- Alert administrators during attacks
- Expose a hackers technique
- Illustrate which vulnerabilities need to be addressed
- Help track down individual hackers

IDS Types

- Network-Based IDS: A network-based IDS (NIDS) uses sensors, which are either host computers with the necessary software installed or dedicated appliances—each with its network interface card (NIC) in promiscuous mode. The NIC driver captures all traffic and passes it to an analyzer to look for specific types of patterns.
- Host-Based IDS: A host-based IDS (HIDS) can be installed on individual workstations and/or servers and watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.

Intrusion Prevention System

The traditional IDS only detects that something bad may be taking place and sends an alert. The goal of an IPS is to detect this activity and not allow the traffic to gain access to the target in the first place.

An IPS is a preventative and proactive technology, whereas an IDS is a detective and after-the-fact technology.

There has been a long debate on IPS and it turned out to be an extension of IDS and everything that holds for IDS also holds for IPS apart for IPS being preventative and IDS being detective.

Physical Control

Physical access control systems (PACS) are a type of physical security designed to restrict or allow access to a certain area or building

Physical security is the protection of the actual hardware and networking components that store and transmit information resources. To implement physical security, an organization must identify all of the vulnerable resources and take measures to ensure that these resources cannot be physically tampered with or stolen.

Physical Control Components

Network Segregation

- Network segregation can be carried out through physical and logical means. A section of the network may contain web servers, routers, and switches, and yet another network portion may have employee workstations.
- Each area would have the necessary physical controls to ensure that only the permitted individuals have access into and out of those sections.

Perimeter Security

- The implementation of perimeter security depends upon the company and the security requirements of that environment.
- One environment may require employees to be authorized by a security guard by showing a security badge that contains picture identification before being allowed to enter a section. Another environment may require no authentication process and let anyone and everyone into different sections.

- Perimeter security can also encompass closed-circuit TVs that scan the parking lots and waiting areas, fences surrounding a building, lighting of walkways and parking areas, motion detectors, sensors, alarms, and the location and visual appearance of a building. These are examples of perimeter security mechanisms that provide physical access control by providing protection for individuals, facilities, and the components within facilities.

Computer Controls

- Each computer can have physical controls installed and configured, such as locks on the cover so that the internal parts cannot be stolen, the removal of the floppy and CD-ROM drives to prevent copying of confidential information, or implementation of a protection device that reduces the electrical emissions to thwart attempts to gather information through airwaves.

Work Area Separation

- Some environments might dictate that only particular individuals can access certain areas of the facility.

Data Backups

Another essential tool for information security is a comprehensive backup plan for the entire organization. Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up. A good backup plan should consist of several components.

- A full understanding of the organizational information resources. What information does the organization actually have? Where is it stored? Some data may be stored on the organization's servers, other data on users' hard drives, some in the cloud, and some on third-party sites. An organization should make a full inventory of all of the information that needs to be backed up and determine the best way back it up.
- Regular backups of all data. The frequency of backups should be based on how important the data is to the company, combined with the ability of the company to replace any data that is lost. Critical data should be backed up daily, while less critical data could be backed up weekly.
- Offsite storage of backup data sets. If all of the backup data is being stored in the same facility as the original copies of the data, then a single event, such as an earthquake, fire, or tornado, would take out both the original data and the backup! It is essential that part of the backup plan is to store the data in an offsite location.
- Test of data restoration. On a regular basis, the backups should be put to the test by having some of the data restored. This will ensure that the process is working and will give the organization confidence in the backup plan.

Cabling

- There are different types of cabling that can be used to carry information throughout a network.
- Some cable types have sheaths that protect the data from being affected by the electrical interference of other devices that emit electrical signals.
- Some types of cable have protection material around each individual wire to ensure that there is no crosstalk between the different wires.
- All cables need to be routed throughout the facility in a manner that is not in people's way or that could be exposed to any danger of being cut, burnt, crimped, or eavesdropped upon.

Control Zone

- It is a specific area that surrounds and protects network devices that emit electrical signals. These electrical signals can travel a certain distance and can be contained by a specially made material, which is used to construct the control zone.

- The control zone is used to resist penetration attempts and disallow sensitive information to "escape" through the airwaves.
- A control zone is used to ensure that confidential information is contained and to hinder intruders from accessing information through the airwaves.
- Companies that have very sensitive information would likely protect that information by creating control zones around the systems that are processing that information

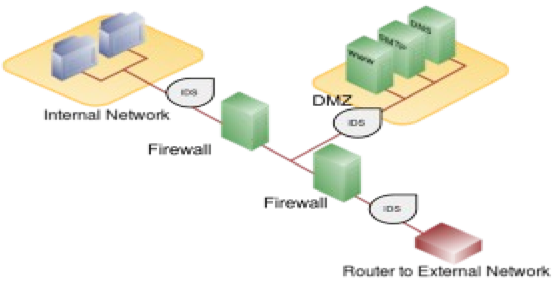
Locked doors

It may seem obvious, but all the security in the world is useless if an intruder can simply walk in and physically remove a computing device. High-value information assets should be secured in a location with limited access.

Firewalls

Another method that an organization should use to increase security on its network is a firewall. A firewall can exist as hardware or software (or both). A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they arrive to a computer. A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria. A firewall may also be configured to restrict the flow of packets leaving the organization. This may be done to eliminate the possibility of employees watching YouTube videos or using Facebook from a company computer.

Some organizations may choose to implement multiple firewalls as part of their network security configuration, creating one or more sections of their network that are partially secured. This segment of the network is referred to as a DMZ, borrowing the term *demilitarized zone* from the military, and it is where an organization may place resources that need broader access but still need to be secured.



Examples of Physical Control

- Fences, Locks, Badge system, Security guard, Biometric system , Mantrap doors, Lighting, Motion detectors, Closed-circuit TVs, Alarms