I. Information Security

History

Information technology is a vehicle that stores & transports information (a Company's most valuable resources) from one business Unit to another.

But what happens if the vehicle breaks down, even for a little while? As businesses have become more fluid, the Concept of Computer Security has been replaced by the Concept of information Security.

Because this new Concepts covers a broader range of issues, from the protection of data to the protection of human resources, information Security is no longer the sole responsibility of a discrete (Seperate) group of People in the Company.

Rather, it is the responsibility of every employee & especially managers.

Organizations must realize that information Security Funding & planning decisions involve more than just technical managers.

Rather the process should involve three distinct gps of decision makers. (or) Communities of interest.

* Information Security managers & professionals
* Information technology managers & professionals.
* Non technical business managers & professionals.

These Communities of interest fulfill the following roles.

* The information ~~Community~~ Security Community protects the organization's information assets from many threats they face.

* The information technology Community Supports the business objectives of the organization by Supplying & Supporting information technology appropriate to the business needs.

* The non technical business Community, articulates & Communicates organizational Policy & objectives & allocates resources to the other groups.

II What is Security?

In general, Security is defined as "the quality or state of being Secure to be free from danger.

Security is often acheived by means of Several Strategies usually undertaken Simultaneously (OR) used in Combination with one another.

Specialized areas of Security.

① physical Security

It encompasses strategies to protect People, physical assets of the workplace from various threats including fire, Unauthorized access (or) natural disasters.

② Personal Security

It overlaps with physical Security in the protection of the people within the organization.

③ Operations Security:

It focuses on Securing the organization's ability to carry out its operational activities without interruption (or) Compromise.

④ Communications Security:

It encompasses the protection of an organization's Communications media, technology & Content & its ability to use these tools to achieve the organization's objectives.

⑤ Network Security:

It addresses the protection of an organization's data networking devices, connections & contents and the ability to use that n/w to complish the organization's data communication fn/s.

⑥ Information Security:

It includes the broad areas of information security, management, computer & data security and n/w security.

Where it has been used.

* Governments
* military
* financial institutions
* hospitals &
* private businesses

Protecting Confidential information is a business requirements.

Information Security Components:

Confidentiality
Integrity &
Availability.

} CIA

CIA Triangle.

CIA has expanded into a more comprehensive list of Critical characteristics of information

At the heart of the study of information Security is the Concept of Policy.

Policy, awarness, training, education & technology are the vital role/Concepts for the protection of information & for keeping information systems from danger.

III. Critical Characteristics of Information:

→ Confidentiality
- Integrity.

→ Availability
- Privacy
- Identification
- Authentication
- Authorization.
- Accountability.

→ Accuracy
- Utility
- Possession.

Confidentiality:

It ensures that only those with sufficient privileges may access certain information.

—When Unauthorized individuals (or) Systems can access information Confidentiality is breached

To protect the Confidentiality of

information, a no. of measures are used

* information Classification
* Secure document Storage
* Application of general Security Policies
* Education of information Custodians and end users.

Ex: a credit card transaction on the Internet.

⇓ by encrypting

Telephone → If the caller is Not authorized

⇓ result

breach of Confidentiality

Integrity:

Integrity means that the data Cannot be modified without authorization

Ex: Integrity is violated when an employee deletes important data files

- when a Computer Virus infects the

Computer, when an employee is able to modify his own Salary in a payroll database,

→ When an unauthorized users Vandalizes (destroy) a website

→ When some one is able to cast a very large number of votes in an online poll & so on.

Availability:

Availability is the characteristic of information that enables user access to information without interference (or) obstruction in a required format.

→ A user in this definition may be either a person (or) another computer system.

→ Availability does not imply that the information is accessible to any user, rather it means availability to authorized users.

→ The information must be available when it is needed.

Ex

High availability systems aim to remain available at all times.

→ Preventing service disruptions due to power outages

→ H/w failures &

→ System upgrades.

Privacy:

The information that is collected, used & stored by an organization is to be used only for the purpose stated to the data owner at the time it was collected.

Identification:

An information system possesses the characteristic of identification when it is able to recognize individual users.

Authentication:

Authentication occurs when a control provides proof that a user possesses the identity that he or she claims.

In Computing e-Business & information Security it is neccesary to ensure that the data transactions, Communications (or) documents are genuine

Authorization:

After the identity of a user is authenticated the user can get the proper authority to access, update or delete the contents of an information asset.

(asset → useful/ valuable quality) benefit (+)

Accountability:

The Characteristics of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person (or) automated process.

For ex

Audit logs that track user activity on an information system provide accountability.

3. Accuray:

Information should have accuray. when it is free from mistakes (or) errors & it has the value that the end users expects.

If information contains a value different from users expectations, it is no longer accurate.

Utility:

Information has value when it serves a particular purpose. This means if information is available.

Possession: ownership

The possession of information security is ~~the state of~~ quality or state of having ownership or control of some object / Item.

IV NSTISSC Security model

National Security Telecommunications & Information Systems Security Committee document

It is now called as the National Training Standard for information Security professionals.

The NSTISSC Security model provides a more detailed perspective on Security.

While the NSTISSC model Covers the three dimensions of information Security, it omits discussion of detailed guidelines & Policies that direct the implementation of Controls.

Another weakness of using this model with too limited an approach is to view it from a Single perspective.

→ The 3 dimensions of each axis become a 3x3x3 Cube with 27 Cells representing areas must be addressed to Secure today's Information systems.

→ To ensure System Security, each of the 27 Cells must be properly addressed during the Security process

For example the interaction b/w technology Integrity & Storage areas requires a Control or Safeguard that addresses the need to use technology to protect the integrity of information while in Storage.

Components of an Information System.

→ S/w

→ H/w

→ data

→ People

→ Procedures

→ Networks.

Software:

S/w Components of IS comprises applications, OS & assorted Command utilities.

S/w Pgms are the Vessels that carry the lifeblood of information through an organization.

These are Created under the demanding Constraints of Project mgmt which limit time cost of manpower.

Hardware:

H/w is the physical technology that houses & executes the S/w stores & Carries the data & provides interfaces for the entry of removal of information from the System.

→ Physical Security Policies deal with H/w as a physical asset & protection from harm (or) theft.

→ Data

Data Stored, processed & transmitted through a Computer System must be protected

→ Data is often the most Valuable asset possessed by an organization

→ The raw, Unorganized, discrete (Separate) (Isolated) potentially useful facts & figures that are later processed (manipulated) to produce the information.

→ People

There are many roles for people in information systems.

- System Analyst
- Programmer
- Technician
- Engineer
- N/w manager
- MIS (Manager of Information System)
- Data Entry operator.

Procedures:

→ A procedure is a series of documented actions taken to achieve something.

→ A procedure is more than a single simple task.

→ A procedure can be quite complex & involved such as performing a backup, shutting down a system, patching s/w.

Networks:

When information systems are connected to each other to form local area n/w (LAN)

These LAN are connected to other n/w such as internet, new security challenges rapidly emerge.

Securing Components

Protecting components from potential misuse & abuse by unauthorized users.

Subject of an attack:

Computer is used as an active tool to conduct the attack.

Object of an attack:

Computer itself is the entity being attack

Two types of attacks:

→ Direct attack

→ Indirect attack.

System

Hacker using a Computer as the Subject of attack

Remote System that is the object of an attack.

1. Direct attack:

When a hacker uses his personal Computer to break into a System

(originate from the threat itself)

2. Indirect attack:

When a System is Compromised & used to attack other system.

[originate from the System / resource that itself has been attacked & is ~~not~~ not functioning or working under the control of a threat)

A Computer Can be both Subject & object of an attack

for ex

first the object of an attack & then Compromised & used to attack other systems.

It becomes the Subject of an attack.

VII Balancing Information Security & Access:

→ Information Security Cannot be an obsolute

→ It is a process

→ not a goal.

→ It should balance protection & availability.

Approaches to Information Security:

* Bottom-up approach

* Top down approach.

→ It has higher probability of success.

→ Project is initiated by upper level manager who issue Policy & procedures & processes

→ It Dictate the goals & expected outcomes of the project.

→ It determines who is Suitable for each of the required action.

SDLC: The Systems Development Life Cycle (SDLC)

SDLC Waterfall methodologies

SDLC is a methodology for the design & implementation of an information System in an organization.

* A methodology is a formal approach to solving problem based on a structured sequence of procedures.

* SDLC consists of 6 phases.

→ Investigation
→ Analysis
→ Logical design
→ physical design
→ Implementation
→ Maintenance & change

Investigation:

It is the most important phase of it begins with an examination of the event or plan that initiates the process.

→ During this phase the objectives, constraints & scope of the projects are specified.

→ At the conclusion of this phase analysis is performed

Analysis:

It begins with the information gained during the investigation ~~process~~ phase.

It Consists of assessments (quality) of an organization, the Status of Current Systems & the Capability to Support the proposed System

→ Analysts begin ~~with~~ by determining what the new System is expected to do & how it will interact with existing Systems.

This phase ends with the documentation of the findings & an update of the feasibility analysis.

Logical design:

In this phase, the information gained from the analysis phase and used to begin creating a systems Solutions for a business problem.

→ Based on the business need, applications are selected that are capable of providing needed Services.

→ Based on the applications needed; then inputs are chosen.

→ In this phase analyst generate no. of alternative Solutions each with

Corresponding Strengths & weakness ~~of~~ and cost & benefits.

✓ At ~~the~~ end of this phase, another feasibility analysis is performed.

4. Physical design:

→ In this phase Specific Technologies are Selected to Support ~~the~~ Solutions developed in logical design

→ The Selected Components are evaluated based on a make (or) buy decision.

→ Final designs ~~are~~ integrate various Components and technologies.

5. Implementation:

→ In this phase, any needed S/w is ~~created~~.

→ Components are ordered, received & tested.

→ Afterwards, users are trained & Supporting documentation created

→ Once all ~~the~~ Components are tested individually ~~they~~ are installed.

Again a feasibility analysis is prepared. & the sponsors are then presented with the system for a performance review & Acceptance test.

6. Maintenance & Change:

→ It is the longest & most expensive phase of the process

→ periodically the system is tested for compliance with business needs

→ Upgrades, updates & patches are managed.

→ When a current system can no longer support the organization, the project is terminated & a new project is implemented.

IX SEC SDLC: The Security Systems Development Life Cycle

The traditional SDLC can be adopted to support the implementation of an information security project.

It includes

- Sec SDLC phases
- Security professionals & the organization
- Key terms in Information Security terminology.

(i) Sec SDLC phases:

Investigation:

This phase begins with a directive from upper mgmt, dictating the process outcomes & goal of the project aswell as budgets and other constraints.

→ This phase begins with an enterprise information Security Policy

→ teams of responsible managers, employees & Contractors are organized.

→ Plans are analyzed

→ Scope of the project as well as Specific goals & objectives are defined.

→ finally organization Feasibility analysis is performed.

Analysis:

In this phase, documents from the investigation phase are Studied.

→ the developed team Conducts a preliminary analysis of existing Security Policies.

→ The risk mgmt task also begins in this phase.

Risk Management:

It is the procan of identifying, assessing & evaluating the levels of risk facing the organization.

Specifically the threaks to the organizations Security & to the information Stored & procesed by the organization.

Logical design:

This phase creates & develops the blueprint for information Security and examines & implements Key Policies

→ Ik team response the incident response action.

→ plans business response to disastky

physical design:

In this phase, Logical design is evaluated

- Alternative Solutions are generated
- Designs for propsed technological Solutions are created
- At the end of this phase, a feasibility study should determine readiness of the proposed project

Implementation:

Similar to traditional SDLC

→ Security ~~Ston~~ solutions are acquired (made), tested, implemented & tested again.

→ Personal issues are evaluated & education pgms are conducted.

→ Finally, the entire tested package is presented to upper mgmt for final approval

Maintenance & change.

Constant monitoring, testing, modification, updating & repairing to meet changing threats have been done in this phase.

2 Security professionals of the organization:

Senior management:

→ CIO: Chief Information officer is responsible for

Assessment
Mgmt &
Implementation of Information Security in the organization

→ Information Security Project team:

Champion

↳ he promotes the projects ensure their supports to both financially & administratively.

→ Team leader:

Understands project mgmt, Personnel mgmt & Information Security technical requirements

→ Security policy developers.

Individuals who understand the organizational Culture & existing Policies

→ Risk assessment Specialists.

Individual who understand financial risk ~~assess~~ assessment techniques.

→ Security professionals:

Trained & well educated specialists in all aspects of Information Security from both technical & Non technical.

→ System Administrators

Administrating the system that house the information used by the organization.

End users → (consume the products)

three types → Data owners
Data custodians
Data users

Data owners:

↳ Responsible for Security & use of a particular set of information

→ Determine the level of data classification
→ Work with Subordinate managers to oversee the day to day administration of the data.

→ Data Custodians:

→ Responsible for the Storage, maintenance & protection of the information
→ oversee data storage & backup
→ Implementing the Specific procedures & Policies

→ Data users: (End users):

Work with the information to perform their daily jobs supporting the mission of the organization.

Everyone in the organization is responsible for the Security of data.

→). Key terms in Information Security terminology:

Asset, Attack, Risk, Security blue print, Security model, threat, threat Agent Vulnerability, Exposure

1) Asset:

An Asset is the organizational resource that is being protected.

An Asset can be logical such as

- website
- information (or)
- data.

An Asset can be physical such as

- person
- Computer System

2) Attack

Attack is an intentional (or) Unintentional attempt to cause damage.

If Someone casually reads sensitive information not intented for his use. This is considered a passive attack.

If a hacker attempts to break into an information system, the attack is considered active

3) Risk:

Risk is a probability that something can happen.

In Information Security it could be the probability of a threat to a System.

4) Security blue print:

It is the plan for the implementation of new Security measures in the organization It is Sometimes called as framework

The blue print presents an organized approach to the Security planning process.

5) Security model:

Security model is a Collection of Specific Security rules that represents the implementation of a Security policies

6) Threats:

A threat is a Category of objects, persons, or other entities that pose a potential danger to an asset.

Pose → Pretend

ex Severe ~~threats~~ storms are also a threat to buildings & their Contents.

Threat Agent:

A threat Agent is the Specific instance (or) Component of a threat.

For ex you can think of all hackers in the world as a Collective threat & Kevin mitnick who was Convicted for hacking into phone Systems, as a Specific threat Agent

Vulnerability:

Weakness or faults in a System or damage are known as Vulnerabilities

Vulnerabilities that have been examined, documented & published are referred to as Well known Vulnerabilities

Exposure:

The exposure of an Information System is a Single instance when the System is open to damage

Vulnerabilities can cause an exposure to potential damage (or) attack from a threat.

II. Security Investigation

I Need for Security

The purpose of Information Security mgmt is to ensure business Continuity & reduce business damage by preventing & minimizing the impact of Security incidents.

* Ensuring that your information remains Confidential & only those who should access that information.
* Knowing that no one has been able to change your information.
  So that you can depend on its accuracy (information Integrity)
* Making Sure that your information is available when you need it
  (By making back-up copies. — off site)

II Business needs first:

Information Security needs four important fn/s for an organization.

* Protects the organization ability to function.

* Enables the Safe operation of applications implemented in the organization IT Systems
* Protects the data ; the organization Collects & uses.
* Safeguards the technology assets in use at the organization.

→ Protecting the functionality of an organization:

Decision makers in organizations must set policy & operate their organizations in Compliance with the Complex & contract the use of technology

→ Enabling the Safe operation of application:

Organizations acquire & operate integrated efficient & capable applications

→ Protecting data that organizations Collect & use.

Protecting data in motion
Protecting data at rest (Storage)

Both are critical aspects of Information Security

The Value of data motivates to steal Sabotage (Destroy) or Corrupt it.

4) Safeguard technology assets in organizations:
— Must add Secure information Services based on the Size & Scope of the enterprise.
→ Need public key infrastructure (PKI)
Integrated System of S/w; encryption methodologies

III Threats:

To protect an organization's information you must

1. Know yourself
— where to store, transport & process.
2. ~~Know~~ Know the threats you face.
— A threat is an object person (or) other entity that represents a constant danger to an asset.

→ Threats to Information Security:

Categories of threats with an examples

(i) Acts of human error (or) failure
— Accidents, employee mistakes.

(ii) Compromises to intellectual property :—

Piracy, Copyright imfringment

(iii) Deliberate acts of espionage or trespass

— Unauthorized accem data collection

(iv) Deliberately acts as information extortion

— Blackmail (or) information disclosure

(v) Deliberately acts of Sabotage or Vandalism

— Destruction of Systems or informations

(vi) Delibrately S/w attacks:

— Viruses, worms, DoS

(vii) Force of nature

— Flood, Fire, earthquake, lightning

(viii) Deviation in QoS:

ISP/WAN Service provider.

(ix) technical H/w failures/errors:

Equipment failures

(x) Technical S/w failures/errors:

Bugs, Code phms, Unknow loopholes

(xi) Technical obsolescence —

Out-dated technologies
(Antiquated)

Threats:

a) Acts of Human error / failure

Making of incorrect assumption
Improper training
Because of inexperience

b) Compromise to Intellectual property:

→ Intellectual property is defined as the ownership of ideas & control over the tangible or virtual representation of those ideas

It includes · trade Secrets
Copy rights
Patents
trademarks

→ Once intellectual property has been defined & properly identified, breaches to IP constitute a threat to the security of this information

→ organization purchases / leases the IP of other organization

→ Most Common IP breaches the Unlawful use (or) duplication of S/w based intellectual property Commonly known as S/w ~~privacy~~ piracy.

→ S/w Piracy affects the world economy

→ US provides approximately 50% of world's S/w

Deliberate Acts of Espionage or Trespass.

Electronic & human activities that can breach the Confidentiality of Information.

→ Attackers can use many different methods to access the information stored in an Information System.

→ Competitive Intelligence
— Use web browser to get Information from market research.

→ Industrial espionage (Spying)

→ Shoulder ~~Surfing~~ Surfing (ATM)
(obtain information from personal Identification number, password & other Confidential by looking over the victim's shoulder.

Trespass: ಅನಧಿಕೃತ / ಅಕ್ರಮ ಪ್ರವೇಶ

Trespassers ~~Can~~ is a Unauthorized users They have not been authorized to enter

Hackers → People who access the information/ S/w Illegally.

There are two Skill level among hackers.

1) Expert hackers: → Masters of Several Pgmming languages, n/working protocols & O/Systems.
2) UnSkilled hackers.

Deliberate acts of Information Extortion (Obtain by force/threat)

Possibility of an attacker/ trusted ~~System~~ insider stealing information from a Computer System

Deliberate acts of Sabotage or Vandalism

Destroy an asset

Damage the image of organization

Cyber terrorism:

Cyber terrorists hack systems to Conduct terrorist activities through n/w (or) internet pathways.

* Deliberate acts of theft:

→ Illegally taking of another's property.

→ Physical theft can be Controlled by installation of alarm Systems.

→ Trained Security professionals.

→ Electronic theft Control is under research

• Deliberate S/w attacks:

Because of malicious code or malicious S/w or Sometime malware.

These S/w Components are designed to damage, destroy or deny Service to the target System

More Common instances are.

Virus
Worms
Trojan horses
Logic bombs
Back doors.

Virus:

Virus transmission is at the opening of Email attachment files

→ Back door (or) trap door:

A Virus or Worm has a payload that installs a backdoor / trap door Component in a (allow unauthorized / attacker) System

which allows attacker to access the System with Special previlages.

Eg: Back Orifice

Polymorphism:

Polymorphic threat is one that changes its apparent shape overtime

These Viruses & Worms actually evolve, Changing their size & appearance to elude (escape / avoid) detection by antivirus S/w Pgms

Virus / Worm Hoaxes (Juggling)

types of Trojan:

- Data sending trojans
- Proxy trojans
- FTP trojans
- Security S/w disabler trojans
- Dos attack Trojans (DOS).

Viruses:

A Pgm or piece of code that be loaded on to your Computer without your knowledge & run against your wishes

Worm:

A Pgm/algm that replicates itself over a Computer n/wd usually performs malicious actions.

Trojan Horse:

Trojan horse don't replicate themselves.

It is destructive Pgm that masquerade (Pretend) as begining appln.

Blended threat:

Blended threats Combine the Characteristics of Virus, Worm, Trojan horse & malicious code with Server & Internet Vulnerabilities.

Antivirus Pgm:

It is a Utility that Searches a hard disk for Viruses & removes any that found.

Macro virus:

Automatically executing macro code Common in Word processors, Spreadsheets & database applications.

Boot Virus:

It infects key operating files located in the Computer's boot Sector.

Worms:

→ A worm is a malicious program that replicates constantly without requiring another program

→ Worms Can Continue replicating themselves until they completely fill available resources such as memory, hard drive space & n/w bandwidths.

Eg MS-Blaster
My Doom
Net Sky are multifaceted attack worms.

→ Once the worm has infected a Computer it can redistribute itself to all e-mail addresses found on the infected System.

~~Worm can deposit the same in the~~ ^ Web Server → Worm can deposit Copies

of itself onto all Webservers that the infected Systems can reach, so that users who subsequently visit these sites become infected.

Trojen Horses attack

Trojen horses arrives via email / Software such as free games

↓

Trojen horse is activated when the S/w or attachment is executed

↓

Trojen horses releases its payload, monitors Computer activity, install back door / transmit information to hacker.

Forces of Nature

- Fire
- Flood
- Earthquake
- Lightning
- Land Slide / Mud Slide — earth & rocks
- Tornado / Server windstorm
- Haricane / typhoon
- Tsunami
- Electro static Discharge
- Dust Contamination

Since it is not possible to avoid force of nature threats, organizations must implement Controls to limit damage.

They must prepare Contigency plans for Continued operations such as disaster recovery plans, Continuity plans & incident respons plans to limit loses in the faces of these threats.

Deviation of QoS.

→ Internet Service Issues

→ Communication & ~~other~~ Service provider issues

→ . Power Irregularities

- Fluctuations due to power
- Power Shortages (excess)
- Power Losses.

→ Technical ~~S~~/w failures / Errors

- Lack of availability
- Unreliable Services
- Some errors are Terminal
- Some errors are intermittent

→ Technical ~~S~~/w Failures

↳ Large quantities of Computer coding are written, debugged

↳ Come from purchasing S/ws ~~are~~ with Unknown hidden faults.

→ Technological obsolescence:
out dated infrastructure can lead Unreliable & Untrustworthy System.

Attacks:

An Attack is an act (or action) that takes advantage of a vulnerability to Compromise Controlled System

It is accomplished by a threat agent that damages or steals an organization's information physical asset.

Vulnerability is an identified weakness in a Controlled System where Controls are not present or are no longer effective.

→ Attacks exists when a Specific act or action Comes into play it may Cause a potential loss.

Malicious Code

The malicious code attack indues the execution of Viruses, Worms, Trojen horses & active web Script with the intent to destroy or Steal information.

Attack replication Vectors

→ IP Scan & attack
→ Web browsing
→ Virus
→ Unprotected Shares.

→ Mass mail.

→ Simple N/w mgmt Protocol (SNMP)

Example.

Hoaxes

Backdoors

password crack

Brute force

↳ The application of Computing

& n/w resources to try every possible Combination of options of a password is called a Brute force attack.

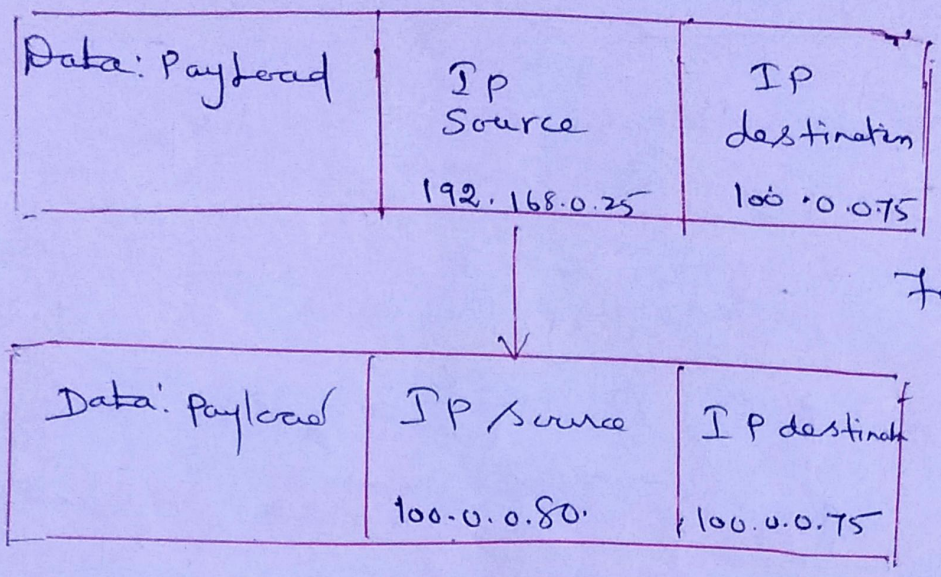
This is often an attempt to repeadly guess pwds to Commonly used accounts, it is Sometimes called a pwd attack.

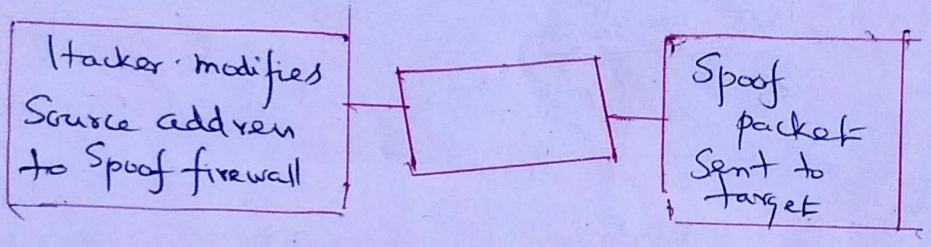
Spoofing:

It is a technique used to gain unauthorized access to Computers.

Intruder Sends msg to a Computer that has an IP address

That indicates that the message are Coming from a trusted host.





Firewall allows packets in, mistaking it for legitimate traffic.

Dictionary:

This is another form of brute force attack noted above for guessing passwords

DoS & DDOS:

→ The attacker sends a large no. of Connection (cl) information request to a target

→ This may result in the system Crashing or unable to perform ordinary fn/s.

DDos is an attack in which a coordinated stream of requests is launched against a target from many location at the same time.

Man in the middle.

It is otherwise called as TCP hijacking attack.

→ The attacker monitors from the n/w; modifies them & inserts them back into the n/w.

→ This type of attack uses IP Spoofing. It allows the attacker to change, delete, reroute add, forge or divert data.

TCP hijacking (session, the Spoofing includes the interception of an encryption key exchange.

SPAM:

→ SPAM is unsolicited (not demanded) Commercial E-mail

→ It has been used to make malicious Code attack more effective

→ Spam is considered as a trivial (injurious or noxious) nuisance

→ It is the waste of both Computer & human resources it causes by the flow of Unwanted E-mail.

Mail Bombing:

Another form of email attack that is also a DoS called a mail bomb.

→ Attacker routes large quantities of e-mail to the target

→ the target of the attack receives Unmanageably large volumes of (annoying) Unsolicited e-mail

Sniffers:

→ A Sniffer is a Program/device that can monitor data travelling over n/w.

→ Unauthorized Sniffers can be extremely dangerous to a n/w's security, because they are virtually impossible to detect

and can be inserted almost anywhere

→ Sniffers often works on TCP/IP n/ws, where they are sometimes called "Packet Sniffers"

Social Engineering:

An attacker gets more valuable information (Convince people to reveal accounts) by calling others & asserting his/her authority by mentioning Chief's name.

Ex: Bank

Buffer overflow:

A buffer ~~error~~ overflow is an appln error that occurs when more data is sent to a buffer than it can handle.

→ Attacker can make the target System execute instructions.

Timing attack:

The attacks allow a web designer to create a malicious form of cookie that is stored on the Client system.

→ The cookie could allow the designer to collect information on how to access password protected sites.

Legal Ethical & professional issues in information Security:

* Law & Ethics in information Security

→ Law are rules that mandate or prohibit certain behaviour in Society. They are drawn from ethics which define Socially acceptable behaviour.

Laws carry the Sanctions of a governing authority &

Ethics do not carry Sanctions of. a governing authority.

Ethics based on Cultural mores

types of Law

- Civil law
- Criminal law
- Tort law
- Private law
- public law

* Relevant U.S Laws General.

→ Privacy
→ Privacy of Customer information
→ Export & Espionage laws
→ US Copyright law
→ Freedom of Information Act of 1966 (FOIA)
→ State & local regulations

* International Laws & Legal bodies

To oversee the range of Security fn/s associated with Internet activities.

→ Digital millennium Copyright Act (DMCA)
→ United nations Charter
→ Policy Versus laws

* Ethical Concepts in Information Security:

→ Cultural differences in Ethical Concepts
→ Ethics & Education

Employees must be trained & kept aware of a no of topics related to Information Security

Proper Ethical & Legal training is vital to Creating an informed, well prepared & low risk System User.

* Deterrence to Unethical & Illegal behaviour:

Deterrance means preventing an illegal or Unethical activity

Laws, Policies & technical controls are examples of deterrence

(vi) Catagories of Controls:

Controlling risk through avoidance, Mitigation or transference may be accomplished by implementing Controls or Safeguards.

Four ways to Categorize Control have been identified.

- Control fn/_
- Architectural layer
- Strategy layer
- Information Security principles

(vii) Feasibility Studies:

Before deciding on the strategy for a specific Vulnerability, all the economic & non economic Consequences of the Vulnerability facing the information asset must be explored.

* Cost avoidance
* Cost Benefit Analysis (CBA) (or) economic Feasibility Study

Confinament Problem

Amount of Benefit = Value of the Information Asset & Value at risk

Single Loss expectancy (SLE)

It is the Calculation of the Value associated with the most likely loss from an attack.

SLE = Asset Value * exposure factor (EF)

Annualized loss expectancy ALE

ALE = SLE x ARO

Cost Benifit Analysis

CBS = ALE (prior) — ALE (post)

— ACS

Bench marking:

An Alternative approach to risk mgt

There are two measures typically used

* Metric based measures
* process based measures

Possible Indicators.

Probable Indicators

Definite indicators

→ Incident Reaction

It consists of actions outlined in the IRP that guide the organization in attempting to stop the incident, mitigate the impact of the incident & provide information for Recovery from the incident.

→ Incident Recovery:

The Recovery process involves much more than the simple restoration of stolen, damaged (or) destroyed data & files

→ Disaster recovery plan: (DRP)

DRP provides detailed guidance in the event of ~~disaster~~ disaster.

DRP must be reviewed during a walk through or talk through on a periodic basis

→ It mitigates the impact of the disaster on the operations of the organization.

5. Business Community plan

It prepares an organization to re-establish Critical business operations during a disaster that affects operations of the organizations during a disaster that affects operations at the primary site.

Developing Continuity Program:

Once the incident response plans and disaster recovery plans are in place, the organization needs to consider, finding temporary facilities to support the continued Viability of the business in the event of a disaster.

Continuity Strategies:

In general there are three exclusive options.

(1) Hot sites
(2) Warm sites
(3) Cold sites

Shared function:

Time-share
Service-bureaus &
Mutual Agreements.

III. Security Analysis

I. Risk Management:

The formal process of identifying & controlling the risks facing an organization is called risk management.

It is the probability of an Undesired event Causing damage to an asset.

There are three steps

→ Risk Identification
→ Risk Assessment
→ Risk Control

→ Risk Identification:

It is the process of examining & documenting the security posture of an organization's information technology.

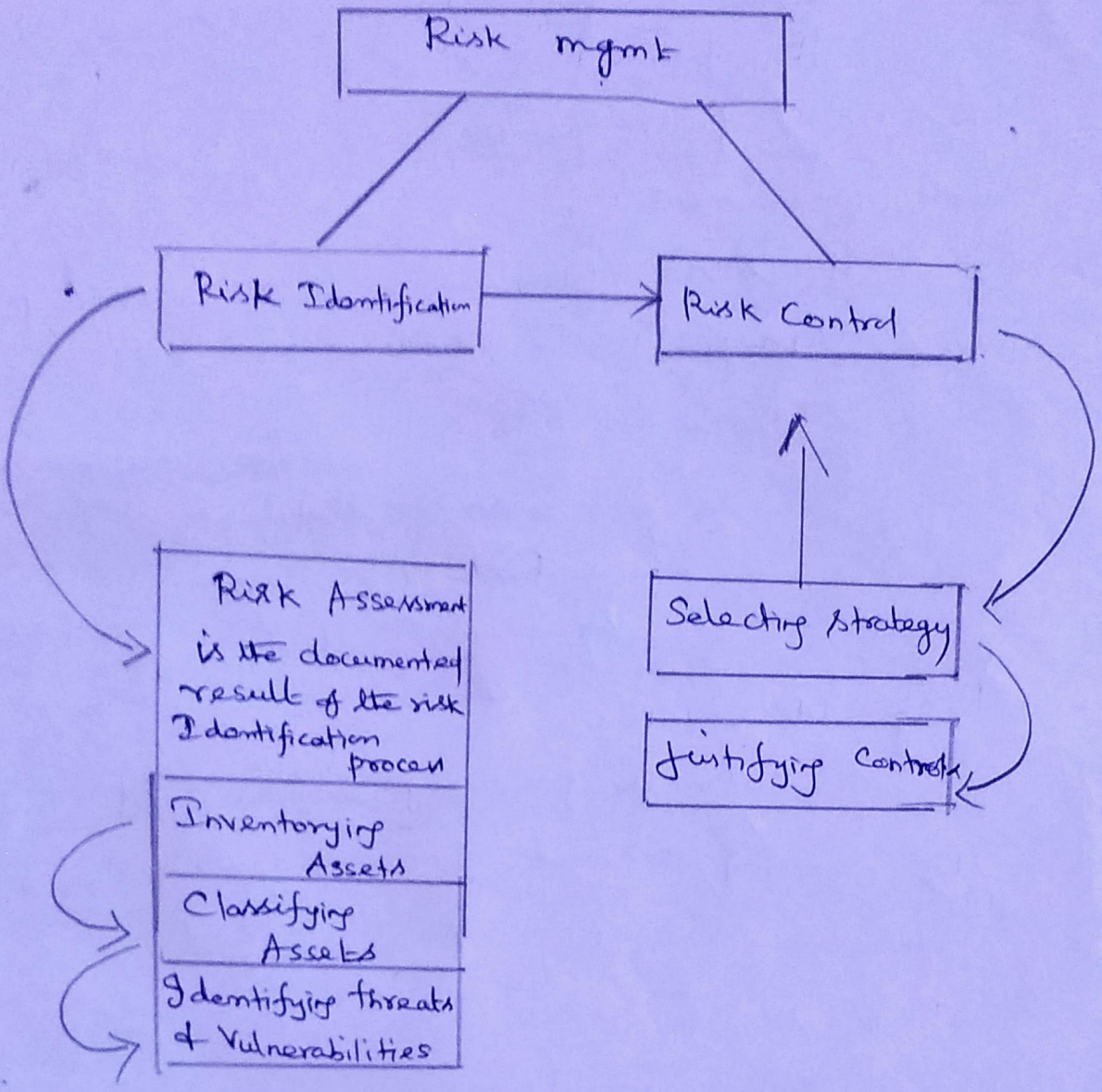
→ Risk Assessment:

It is the documentation of the result of risk Identification.

→ Risk Control:

It is the process of applying controls to reduce the risk to an organization's data & Information systems

Components of Risk management:



An overview of Risk mgmt:

Over 2,400 years ago by Chinese General Sun Tzu said

(1) If you know the enemy & know yourself, you need not fear the result of a hundred battles.

2) If you know yourself but the enemy, for every victory gained, you will suffer a defeat

3) If you know neither the enemy nor yourself, you will succumb in every battle.

Know yourself

→ Identify, Examine & understand the Information Systems.

→ To protect assets, you must understand what they are?. How they add Value to the organization & which Vulnerabilities they are susceptible.

→ Policies, Education & training Pgms & technologies that protect information must be carefully maintained & administered to ensure that they are still effective.

Know the enemy:

Identifying, Examining & Understanding the threats facing the organization

* The Roles of the Communities of Interest.

It is the responsibility of each Community of interest to manage the risks.

* Information Security:

Understand the threats of attacks that introduce risk into the organization.

→ take a leadership role in addressing risks.

* Mgmt & Users:

Mgmt must ensure that Sufficient resource are allocated to the information security & technology gps to meet the security needs of the organization.

→ Users work with the systems & the data

* Information technology:

→ It Must build Secure Systems & operate them Safely.

→ Important Risk factors of Information Security are

→ Understand the threats & attacks of the organization

→ taking asset inventory.

→ Verify the threats & vulnerabilities.

→ Review the Cost effectiveness of various risk control measures.

II Risk Identification:

IT professionals to know their organization's information assets through Identifying, Classifying & prioritizing them.

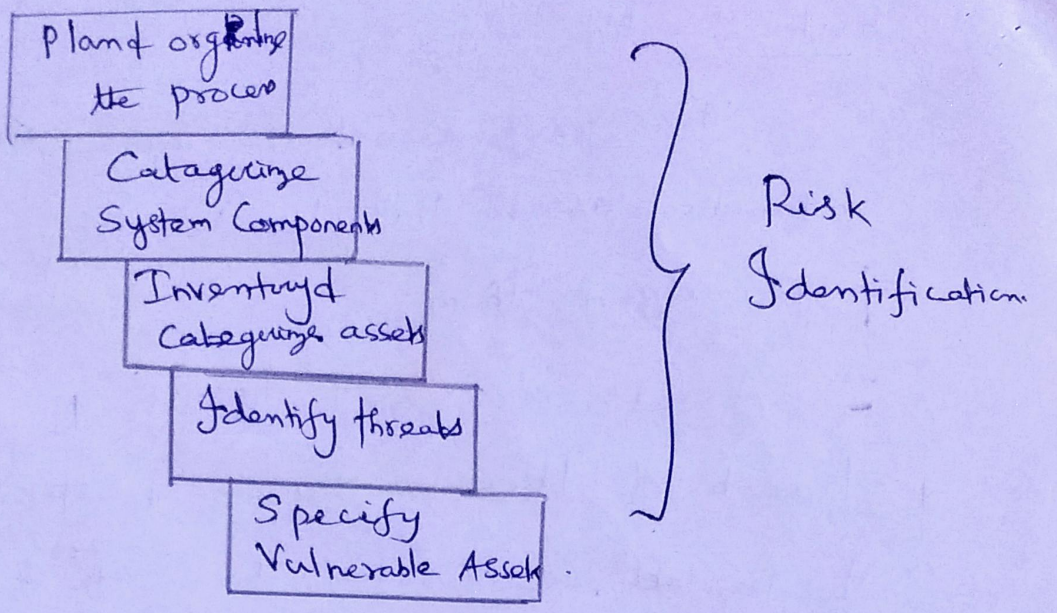
→) Assets are the target of various threats & threat agents & the goal is to protect the assets from the threats.

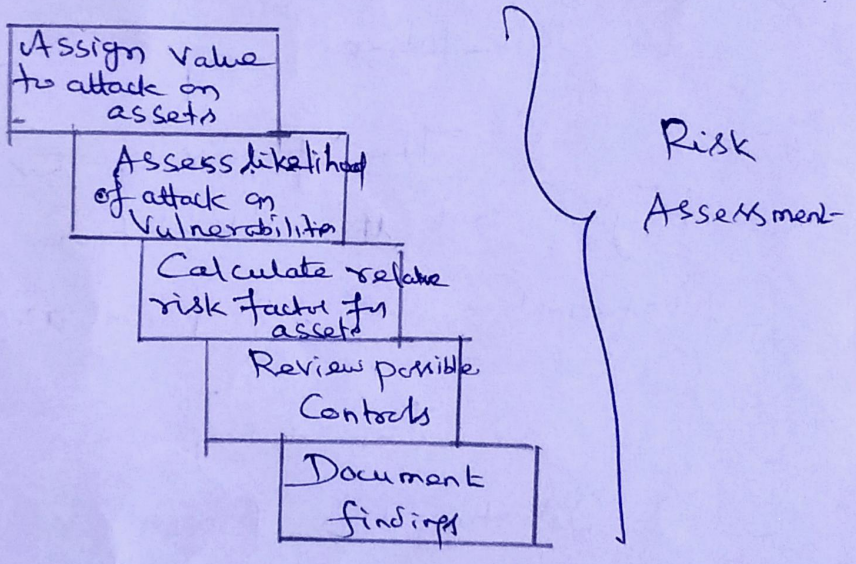
Once the organization assets have been identified, a threat identification process is Undertaken.

The process of Risk Identification begins with the identification of the organization's information assets & an assessment of their value.

The Components of the Risk Identification process is shown in the following figure.

Here also ~~from~~ we are going to discuss about how to mitigate the Vulnerabilities (or) risks.





1. Asset Identification & Valuation:

It Includes all the elements of an Organizations System, such as People; Procedures data & information, S/w, H/w & networking elts.

① Components of Information System

Categorization of IT Components

→ People
→ Procedures
→ Data
→ S/w
→ H/w

② People, procedures & Data Asset Identification

③ H/w, S/w & N/w Asset Identification

④ Automated Risk mgmt tools

(ii) Information Asset Classification

Three kinds of classifications are.

Confidential data

Internal data &

public data

(iii) Information Asset Valuation:

Sample Inventory worksheets are as follows.

System Name : SLS e-Commerce

Date Evaluated : February 2018

Evaluated by : Dr. P. KRISHNA KUMAR

Information Assets	Data Classification	Impact to profitability

(iv) Data classification:

Confidential.

Internal

External

Confidential

Access to information with this classification is strictly on a need to know basis or as required by the terms of a Contract.

Internal: Internal information does not meet the criteria for the Confidential Category

External:

All information that has been approved by management for public release.

The military uses five level classification

→ Unclassified data
→ Sensitive but Unclassified data
→ Confidential data
→ Secret data
→ Top Secret data

Organization may use

→ public data, → advertisement
→ for office use only → Internal Communication
→ Sensitive data → loss
→ Classified data → well being of an organization

Organization may have

Research data
Personal data
Customer data &
General Internal Communication

IV Security Clearances:

The other side of the data classification

Scheme is the personal Security Clearance structure.

Each user of data must be assigned a single authorization level that indicates the level of classification he/she is authorized to view

Eg Data Entry clerk
development programmer
Information Security Analyst / CIO

→ Management of a classified data.

This includes storage, portability distribution & destruction.

→ Each classified document should contain the appropriate designation at the top & bottom of each page.

Dumpster Diving:

To retrieve information that could embarrassing (degrade) a Company (or) Compromise information Security.

(V) Threat Identification:

After Identifying the information assets the analysis phase moves on to an examination of the threats facing the organization.

* Identify & prioritize threats & threat agents

Threat	Example
* Act of human error or failure	Accidents. employee mistakes
* Compromises to intellectual property	Piracy, copyright infringement
* Deliberate S/w attacks	Viruses, worms, macros, DOS
* Forces of nature	Fire flood, lightning earthquake
& soon.	

(VI) Vulnerability Identification:

→ Create a list of Vulnerabilities for each information asset.

→ Group of People interactively in a series of Sessions give best result

→ At ~~the~~ end of ~~the~~ identification process you have a list of assets & their ~~Vulnerabilities~~ Vulnerabilities.

III Risk Assessment:

Assigns a risk rating or score to each information asset.

It is useful in gauging the relative risk to each Vulnerable asset.

It can be Categorized as

(1) Valuation of Information Assets
(2) Likelihood
(3) Risk determination
(4) Identify possible Controls
(5) Documenting the results of Risk assessment

(1) Valuation of Information assets:

→ Assign weighted scores for the value to the organization of each Information asset.

→ National Institute of Standards & Technology gives some Standards

→ To be effective the Value must be assigned

2 Likelihood:

It is the probability of Specic Vulnerability within an organization will be succesfully attacked.

→ NIST gives some standards

→ 0.1 = Low

1.0 = High

Ex No. of n/w attacks can be forecast based on how many n/w address the organization has assigned.

3) Risk Determination:

Risk = [(Likelihood of Vulnerability occurence) × (Value of Information Asset)] — (% of risk mitigated by Current Controls) + Uncertainity of Current Knowledge of the Vulnerability.

for the purpose of relative risk assessment, risk equals.

— likelyhood of Vulnerability Occurance

TIMES Value

— MINUS % risk already Controlled

— PLUS an elmt of Uncertainty.

Ex

Information Asset A has a Value Score of 50 & has one Vulnerability. Vulnerability 1 has a likelihood of 1.0 with no Current Controls estimate that assumptions & data are 90% accurate.

Soln

$$\text{Risk} = [(1.0) \times 50) - 0\% + 10\%$$

$$= (50 \times 1.0) - ((50 \times 1.0) * 0.0) + (50 \times 1.0) \times 0.1)$$

$$= 50 - 0 + 5$$

$$= 55$$

(8) a

Access Controls

→ Specially addresses the admission of a user into a trusted area of the organization.

→ ex
Computer rooms
Power rooms.

→ Combination of Policies, Pgms & technologies

Types of Access control:

MACs → Mandatory Access control
Give users & data owners.
Limited Control over access to Information resources.

DAC : Discretionary Access Control
Variation of MAC users are assigned matrix of authorizations for particular area of access

Non Discretionary Control:
Managed by a Central authority in the organization.

4) Identify possible Controls (for Residual Risk)

→ Residual risk is the risk that remains to the information asset even after the existing control has been applied

three general categories of controls

1. Policies
2. Pgms
3. Technologies.

Policies:

→ General Security Policy
→ Program Security Policy
→ Issue Specific Policy
→ Systems Specific Policy

Programs:

→ Education
→ Training
→ Awarness

Security technologies

→ technical implementation Policies

Lattice-based Access Control.

Variation of MAC - users are assigned matrix of authorizations for particular areas of access.

Documenting the Results of Risk Assessment:

By the end of Risk Assessment process, we probably ~~we have a~~ have a Collection of long lists of Information assets with data about each of them.

→ The goal of this process is to identify the information assets that have Specific Vulnerabilities & list them, ranked according to those most needing protection.

The final summarized document is the ranked Vulnerability risk worksheet, a sample of which is shown in the following table. The following table represents the Ranked Vulnerability risk ~~the~~ worksheet.

Asset	Asset impact	Vulnerability	Vulnerability likelihood	Risk Rating factor
* Customer service request via email (inbound	55	Email disruption due to H/w failure	0.2	11
* Customer order via SSL (in bound)	100	Lost orders due to web Server H/w failure	0.1	10
* Customer order via SSL (inbound	100	Lost order due to web Server or ISP Service failure	0.1	10
* Customer Service Request via email (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
* Customer order via SSL (inbound) SSL - Secure Socket Layer.	100	Lost orders due to web Server S/w failure	0.01	1

IV Risk Control Strategies of Information Flow

There are four Strategies to Control the risk from these Vulnerabilities

1. Apply Safeguards .. (Vulnerability Avoidance)
2. Transfer the risks to other areas (Transference)
3. Reduce the impact should the Vulnerability be exploited (mitigation)
4. Understand the Consequences & accept the risk without control or mitigation (Acceptance)

a) Avoidance.

It is the risk Control Strategy that attempts to prevent the exploitation (Engaging overwork) of the Vulnerability.
↳ (manipulate to one's advantage)

three Common methods of risk avoidance are

→ Appln of Policy
→ Appln of training & Education
→ Application of technology

b) Transference:

Transference is the Control approach that attempts to shift the risk to other Other assets, Other processes or Other organizations.

It may be accomplished through rethinking how Services are offered, revising deployment models, outsourcing to Other organizations or purchasing Insurance

Top 10 Information Security mistakes made by individuals

1. pwd on post it - Notes.
2. Leaving Unattended Computers on
3. opening e-mail attachments from Strangers
4. Poor pwd etiquette
5. Laptops on the loose
6. ~~Blabbette~~ Blabber ~~mouths~~ mouths
   ↳ People who talk about pwds
7. Plug & Play

8. Unreported Security Violations

9. Always behind the times

10. Not watching for dangers inside the organization

(iii) Mitigation :

It is the Control approach that attempts to reduce the impact caused by the exploitation of Vulnerability through planning & preparation.

→ Mitigation begins with the early detection that an attack is in progress & the ability of the organization to respond quickly, efficiently & effectively.

It ~~includes~~ includes 3 types of plans

1. Incident Response plan - IRP

Action to take while incident is in progress

2. Disaster recovery plan (DRP) :
Most common mitigation procedure.

3. Business Continuity plan: (BCP):

Continuation of business activities if catastrophic event occurs

(iv) Acceptance:

It is the choice to do nothing to protect a Vulnerability & do accept the outcome of its exploitation

This strategy occurs when the organization has

→ Determined the level of risk
→ Assessed the probability of risk
→ Estimated the potential damage
→ Evaluated the control
→ Decided that the particular fn/-; Service, information & asset

(v) Selecting a Risk Control Strategy:

Level of threat & value of asset play major role in selection of strategy.

IV Logical Design

I Information Security Policy
Planning for Security

Information Security program begins with creation and/or review of Organization's information Security Policies, Standards & practices.

IS Blueprint Creates plan for future Success.

Why Policy?

→ A quality information Security program begins & ends with Policy.

→ Policies are least expensive means of Control & often the most difficult to implement

Some basic rules must be followed when Shaping a Policy

→ Never Conflict with law

→ Stand up in Court

→ Properly Supported & administered

→ Contribute the Succes of the organizati on.

→ Involve endusers of infumation Systems

Definitions:

Policy :

This is the Course of action used by an Organization to Convey instructions from mgmt to those who perform duties.

→ Organizational rules for acceptable / Unacceptable behaviour

→ Penalities for violations

→ Appeal procen

Standards:

More detailed steps of what must be done to Comply with policy.

Practices / procedures & guidelines explain how to Comply with policy.

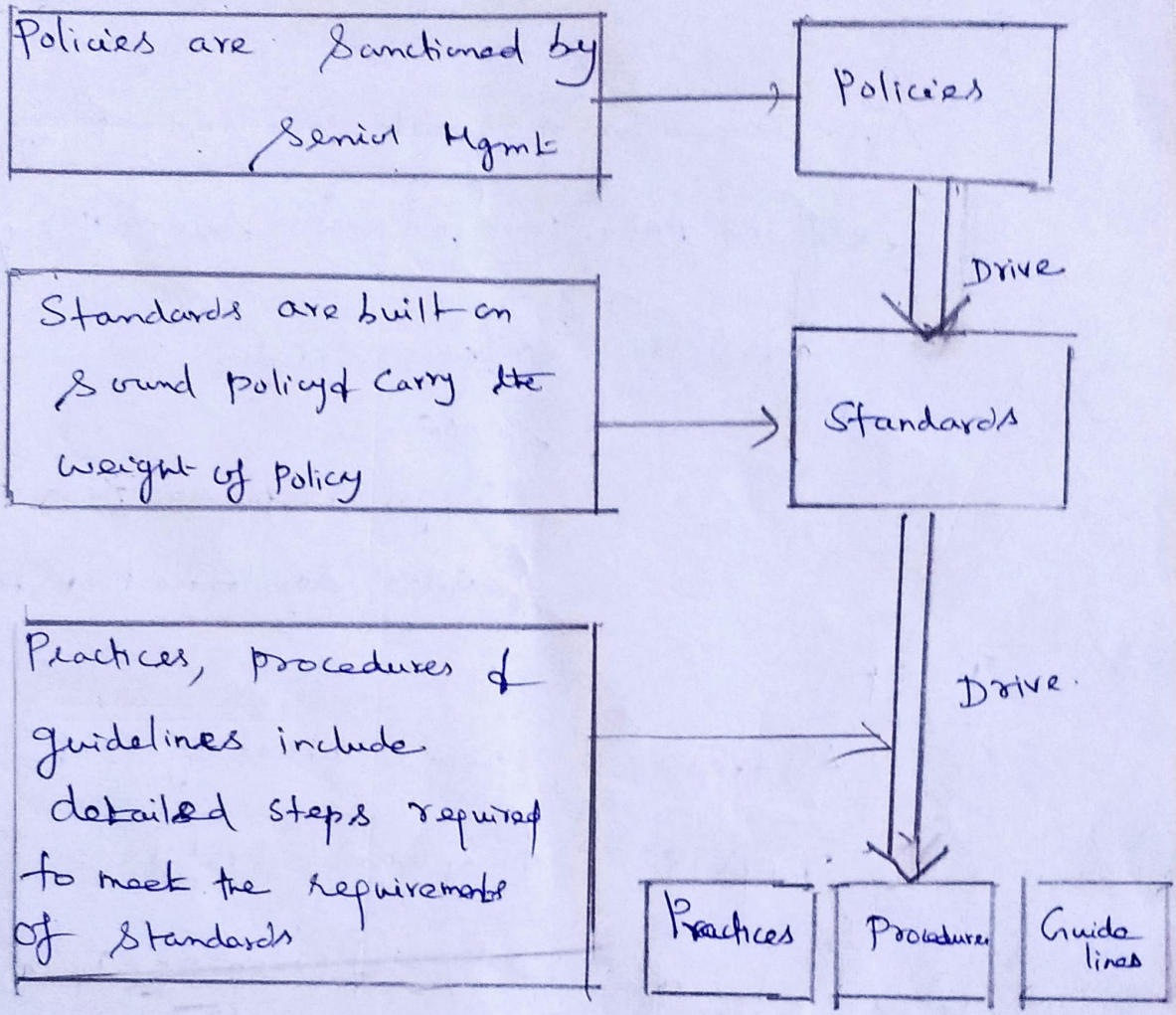
For a Policy to be effective It must be

Properly disseminated

Read

Understood

Agreed to by all members of organization



2. types of Policies

EISP → Enterprise Information Security Program.

ISSP → Issue - Specific Information Security Policy.

SysSP → System - Specific Information Security Policy.

EISP :

Also known as general Security Policy, IT Security Policy or information Security Policy.

→ Sets the Strategic direction
Scope
Assign responsibilities &
Guides development & Implementation

ISSP

Addresses specific areas of technology.
requires frequent updates.

Approaches to creating & managing ISSP.

This could include

Email
Use of Web
Worms
Viruses

3. System Specific Policy (Sys SP)

It falls into two gps.

Access Control lists &
Configuration rules

ACL Policies: (Access Control lists)

Both micro Soft windows & Novell Netware 5.x/6.x families of systems translate ACLs into sets of configurations that administrators use to control access to their respective systems.

ACLs regulate

→ Who can use the System
→ What authorized user can access
→ When authorized users can access the System
→ Where authorized user can access the System from
→ How authorized users can access the System.

II The Information Security Blue print:

→ It is the basis for the design, Selection & implementation of all Security Policies, education & training programs & Technological Controls

→ More detailed version of Security framework, which is an outline of overall

information Security Strategy for organization &
a road map for planned changes to the organization
Information Security Environment of the organization

→ Should also serve as a scalable, upgradable
↓ Comprehensive plan for the information Security
needs for coming years.

(iii) Standard & practice — Security models.

1* ISO 17799/BS 7799

This is one of the most widely referenced & often discussed Security models is the information technology — Code of practices for Information Security mgmt.

* In 2000 this code of practice was adopted as an international Standard framework for information Security by the International organization for Standardization (ISO) & the International Electrotechnical Commission (IEC) as ISO/IEC 17799.

2. Drawbacks of ISO 17799/BS7799.

Several Countries ~~have~~ not adopted 17799 Claiming there are fundamental problems.

→ The global information Security Community has not defined any justification for a Code of practice as identified in the ISO/IEC 17799.

→ 17799 lacks "the necessary measurement precision of a technical Standard.

→ 17799 is not as Complete as ~~Other~~ frameworks available.

(iii) 3. Objectives of ISO 17799

Organizational Security Policy is needed to provide mgmt direction & Support.

(iv) Ten Sections of ISO/IEC 17799

→ Organizational Security Policy

→ Organizational Security Infrastructure.

→ Asset Classification & Control.

→ Personal Security

→ physical & Environmental Security.

→ Communications & Operations Mgmt

→ System Access Control

→ System Development & Maintenance

→ Business Continuity planning.

→ Compliance.

Alternate Security models available Other than ISO 17799 / BS 7799.

IV NIST Security models:

This refers to "The National Security telecommunications & Information Systems Security Committee document.

This model Consists of 3 dimensions

The following NIST documents can assist in the design of a Security framework.

NIST SP 800-12

NIST SP 800-14

NIST SP 800-18

NIST SP 800-26

NIST SP 800-30

→ Risk mgmt for IT Systems

→ NIST Special publication SP 800-12

↳ It provides little guidance

→ NIST Special publication SP 800-14

↳ It provides best practices of security principles

→ NIST SP 800-18 :

It provides detailed methods for assessing & implementing controls & plans for applns for varying size.

→ It can serve as a useful guide to activities

→ The following contents for publication 800-18

System boundaries

multiple & similar Systems

System categories

→ Plan Development

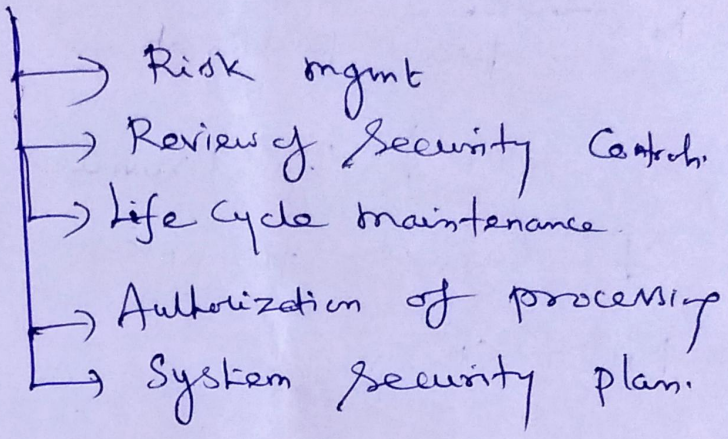
→ Management Controls

→ Operational Controls

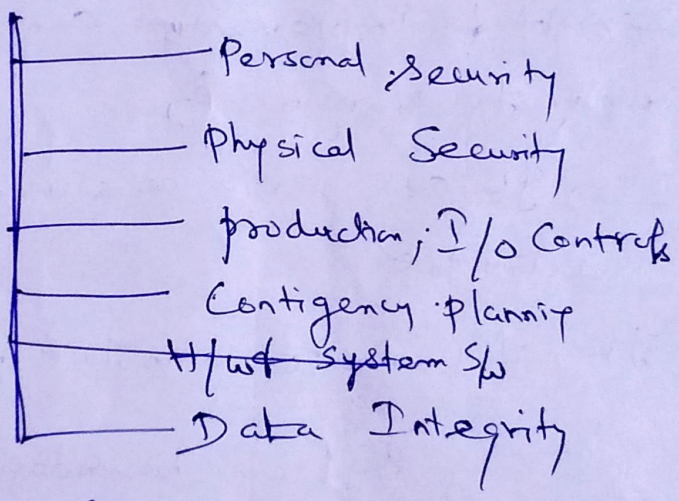
→ Technical Controls

4) NIST SP 800-26 Security Self assessment Guide for IT Systems.

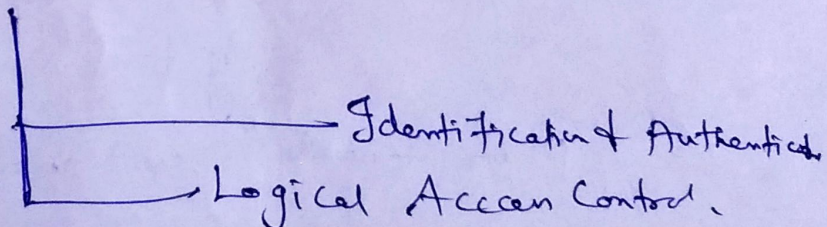
Mgmt Controls



Operational Controls.



Technical Controls



V Visa International Security model:

It measures, Strong Security measures in its business associates & has established guidelines for the Security of its information systems.

It has developed 2 important documents.

1. Security Assessment process
2. Agreed upon procedures.

Both document provide Specific instructions on the use of the VISA Cardholder information Security Pgms.

→ Using these document, a Security team can develop a Sound Strategy for the design of good Security architecture.

- Baseling of Best Buriness practices:

These are the, Solid methods for Collecting Security practices, but provide less detail than a Completete methodology.

- The Federal Agency Security practices (FASP) site (fasp.nist.gov) designed to provide

best practices for public agencies & adapted easily to private institutions.

The document found in this site include specific examples of key policies & planning documents, Implementation Strategies for key technologies & position description for key Security personnel.

Pgm mgmt includes the following

→ A Summary guide:

public law / executive orders &

Policy document.

→ Position description for Computer System Security officer.

→ for Computer Specialists

→ for information Security officer.

→ Sample of an Information technology for a large service application

→ Program, policy ...

→ hand book & Stand OS procedures

→ Tele communication mobile computer ~~Ani~~ Policy.

VI. Design of Security Architecture.

→ Hybrid frame work for a Blue print of an information Security Systems

→ Sphere of protection

→ Level of Controls

- Mgmt Controls
- Security Controls &
- Technical Controls

→ Defense in Depth

→ Security perimeter

→ Key technology Components.

- Firewall
- gateway router
- Firewall Subnet
- Demilitarized Zone (DMZ)

↳ It is a no-man land, b/w the inside & outside n/ws where some organizations place web Servers.

These Server provides accen to organizations web Pages without allowing web request to enter the internal n/ws

Proxy Server:

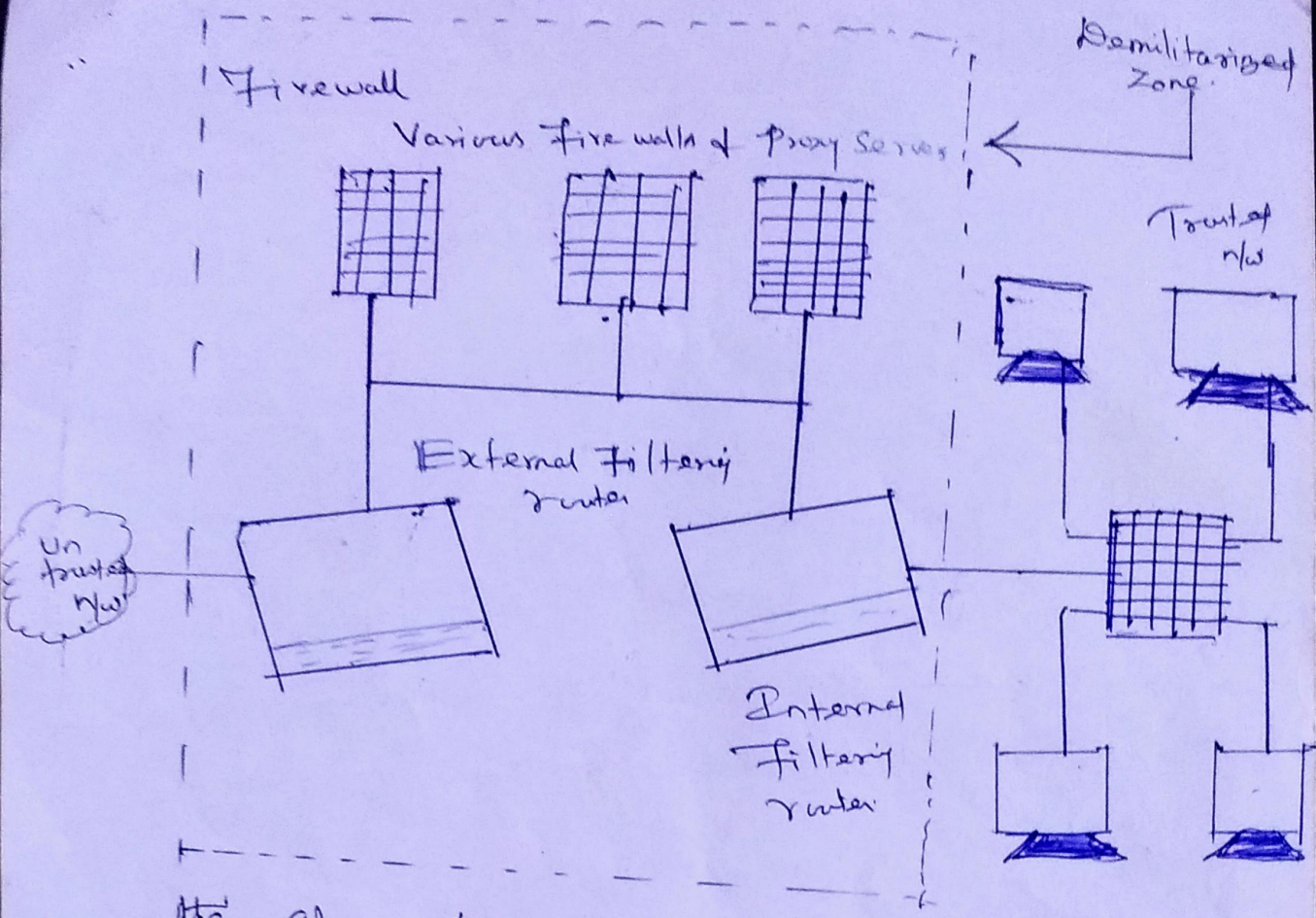
is an alternative approach to the disadvantages of using a firewall subnet or a DMZ is to use a proxy server (or) proxy firewall

When an outside client requests a particular web page the proxy server receives the request as if it were the subject of the request; then asks for the same information from the true web server. (acts as a proxy for the requester) & then responds to the request as proxy. for the true web server.

For more frequently accessed webpages proxy servers can Cache or temporarily store the page & these are sometimes called Cache Servers.

Intrusion Detection Systems: (IDS)

In an effort to detect Unauthorized activity within the inner n/w or an individual m/cs an organization may wish to implement Intrusion Detection Systems (or) IDS.



the above figure depicts the firewall proxy Servers & DMZs

IDS come in two versions.

→ Host based &

→ N/w based

Host based IDSs: are usually installed on the machines they protect. to monitor the status of Various files stored on those m/cs

6. N/w based IDs:

look at patterns of n/w traffic & attempt to detect Unusal activity based on previous baselines

This could include packets coming into the organization's n/ws with addresses from n/cs already within the organization (IP spoofing)

It could also include high volumes of traffic going to outside addresses (as in the case of data theft) or coming into the n/ws (as in a DOS attack).

Both host & n/w based IDS require a database of previous activity.

7. Security Education, training & Awareness Pgm.

As soon as general Security policy exists, Policies to implement Security education, training & Awareness (SETA) Pgm follow

SETA is a Control measures designed to reduce accidental Security breaches by employees.

Security education & training builds on the

.. General knowledge the employees must possess to do their jobs, familiarising them with the way to do their jobs Securely

→ The 'SETA' pgm Consists of three elements Security education, Security training & Security awarness.

The purpose of SETA is to ~~the~~ enhance Security by

→ improving awarness of the need to protect System resources

→ Developing Skills & knowledge so Computer users can perform ~~their~~ jobs more Securely.

→ Building in depth knowledge, as needed, to design, implement or operate Security programs for organizations & Systems.

Security Education:

Every one in an organization needs to be trained & aware of information Security but not every member of an organization needs a formal degree or Certificate in information Security

Security training:

It involves providing members of the Organization with detailed information & hands on instruction to prepare them to perform their duties Securely.

Mgmt of Information Security can develop Customized in-house training or outsource the training Pgm.

Security Awarness:

One of the least frequently implemented but most beneficial pgms is the Security awarness program.

→ Designed to keep information Security at the forefront of user's mind

Need not be Complicated or expensive.

If the program is not actively implemented, employees may begin to tune out & risk of employee accidents & failures increases.

VII Contigency: (Planning for continuity).

Contigency planing Comprises a set of plans designed to ensure the effective

. reaction & recovery from an attack & the subsequent restoration to normal modes of business operations

→ organizations need to develop disaster recovery plans, incident response plans & business continuity as subsets of an overall CP.

An incident response plan (IRP) deals with the identification, classification, response & recovery from an incident. but if the attack is disastrous (ex fire, flood, earthquake) the process moves on to disaster recovery & BCP

→ A business Continuity plan (BCP) ensures at critical business functions continue, if a catastrophic incident or disaster occurs. BCP occurs concurrently with DRP when the damage is major or long-term, requiring more than simple restoration of information & information resources.

Components of Contigency planning:

There are six steps to Contigency planning

→ Identifying the mission or business critical fn/s

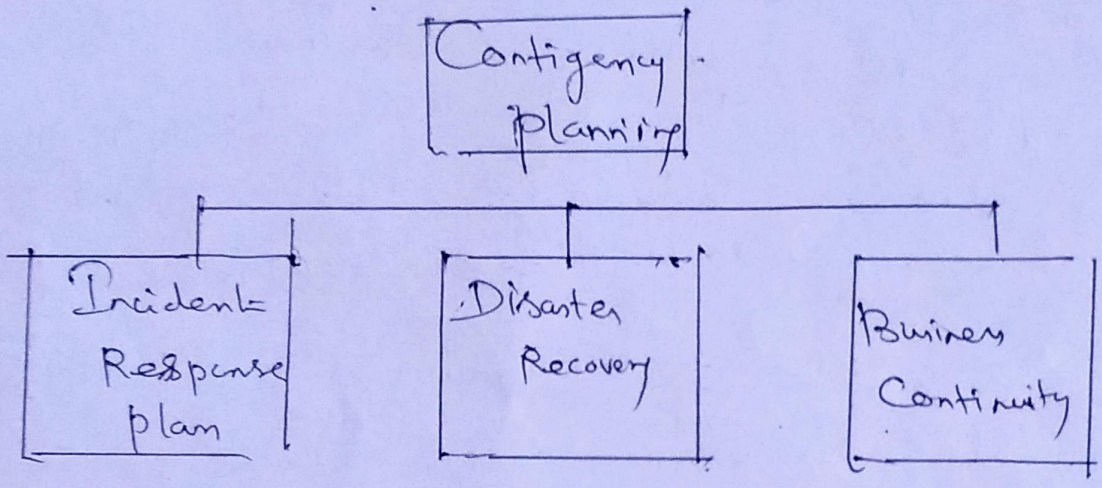
→ Identifying the resources that support the critical fn/s

→ Anticipating Potential Contigencies or disasters.

→ ~~Sele~~ Selecting Contigency Planning Strategies

→ Implementing the Contigencies Strategies of

→ Testing & revising the Strategy.



* Buriness Impact Analysis: (BIA)

A BIA is an investigation & assessment of the impact that various attacks can have on the orgenization.

The Contigency team conducts the BIA

BIA ~~is~~ in the following Stages

* threat attack identification & prioritization
* Analysis
* Succes Scenario development

Incident Detection:

Incident Detection relies on either a human or automated System, which is often the help desk staff, to identify an Unusual occurance & to classify it properly as an incident

Incident classification:

It is the process of examining a potential Incident

Incident Candidate:

Determining whether (or) not the Candidates Constitutes an actual incident

Incident Indicators:

There is a no. of occurances that Could Signal the presence of an incident Candidate.

Donald Pipkin, an IT Security expert identifies 3 Catagories of incident indicators possible, probable & Definite indicators

4 types of possible indicators of events

— damage Assessment

→ Subordinate plan Classification.

3 Incident response plan (IRP):

It is the Set of activities taken to plan for, detect & Correct the impact of an incident on information assets.

IRP Consists of the following 4 phases.

- Incident Planning
- Incident Detection
- Incident Reaction
- Incident Recovery

Incident Planning:

→ Planning for an incident is the first step in the overall process of incident response planning.

→ The planners should develop a Set of documents that guide the actions of each involved individuals who reacts to & recovers from the incident

V physical Design

I Security technology:-

Security is a quality (or) state of being secure - to be free from danger.

A successful organization should have multiple layers of security in place.

→ physical security
→ personal security
→ Operations security
→ Communications security
→ N/w security
→ Information security

physical design:

It is made up of two parts

→ Security technologies
→ physical security

physical design process:

→ Identifies Complete technical solns based on these technologies

→ Design physical security measures to support the technical solns.

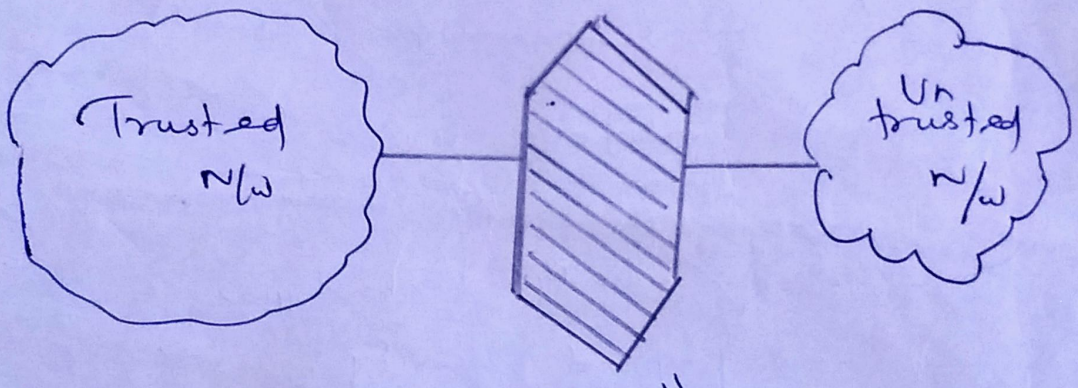
Firewalls:

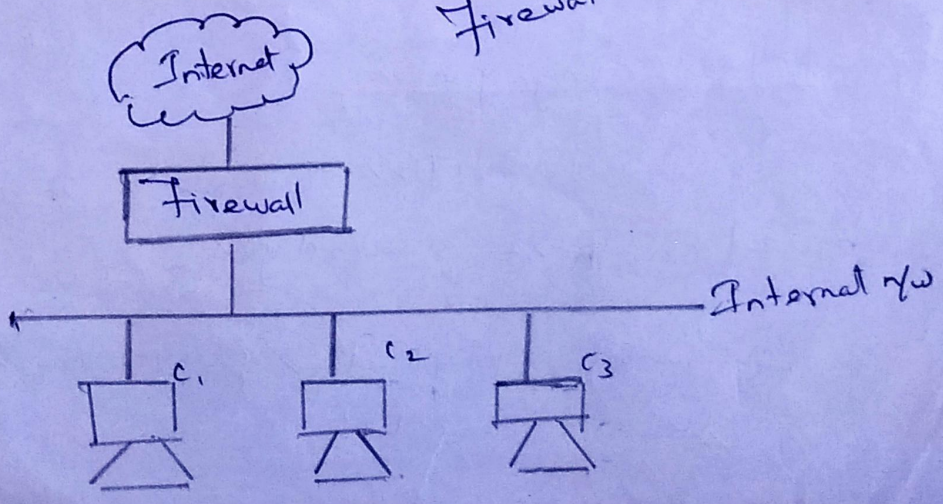
A S/w or H/w Component that restricts n/w Communication b/w two Computers / N/ws

In buildings ; a fire wall is a fireproof wall that restricts the spread of a fire.

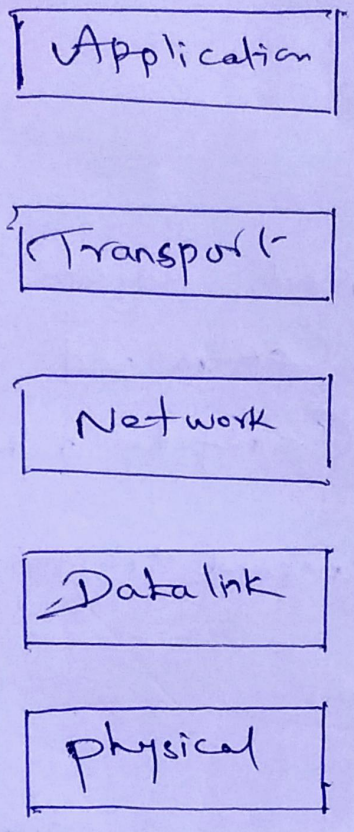
→ N/w firewall prevents threats from spreading from one n/w to another

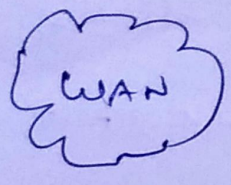
Internet firewall

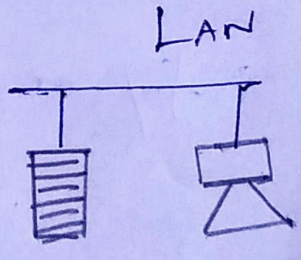




Internet protocol Stack.







What firewalls do

It protects the resources of an internal h/w

* Restrict external Accem
* Log n/w activities.

— IDS
— DoS

↳ Act as an Intermediary
↳ Centralized Security mgnt
↳ Carefully administer one firewall

to Control internet traffic of many m/cs

firewall types

firewall categorization methods

(is fn/ or methodology the Firewall use.

five processing modes that firewall Can be Categorized.

(1) Packet Filtering
(2) application gateways

3. Circuit gateways
4. MAC layer firewalls.
5. hybrids.

→ Packet (firewalls) filtering:

→ Examine the header information of data packets that come into a n/w

→ It Installed on TCP/IP based n/w

→ If device finds a packet that matches a restriction it stops the packet from traveling from one n/w to another.

main strengths: Speed & flexibility.

→ three Subsets of packet filtering firewa

Static filtering
dynamic filtering
Stateful Inspection.

(i) Static Filtering

↳ how the firewall decides which pkts are allowed & which are denied

It is common in n/w routers & gate ways.

(ii) Dynamic Filtering:

It deals with event

Positive → Internal user to engage specific activity upon request

Negative → dropping all pkts from a particular address

(iii) Stateful Inspection:

All modern firewalls today in the market today are stateful

It performs using state table.

Stateful Inspection Firewall

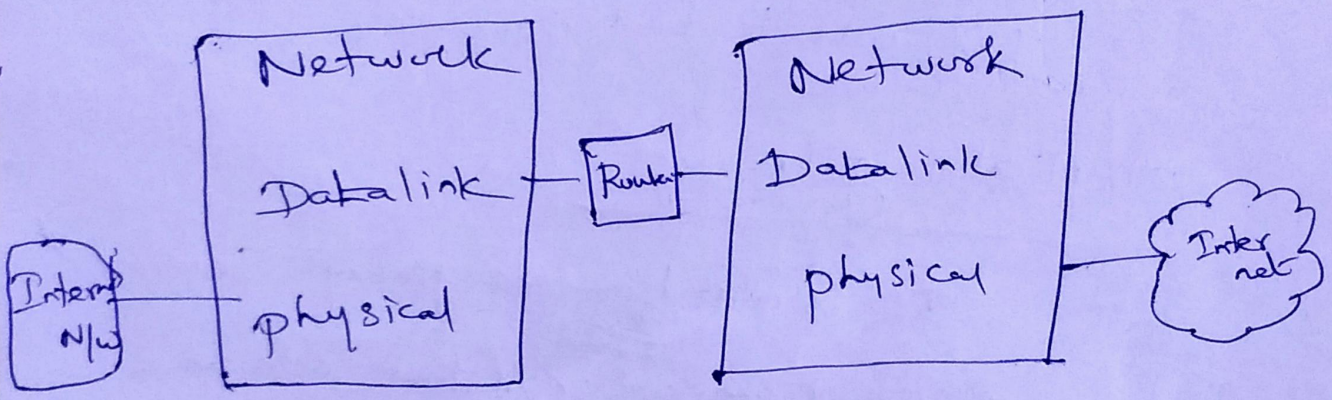
Firewall Router

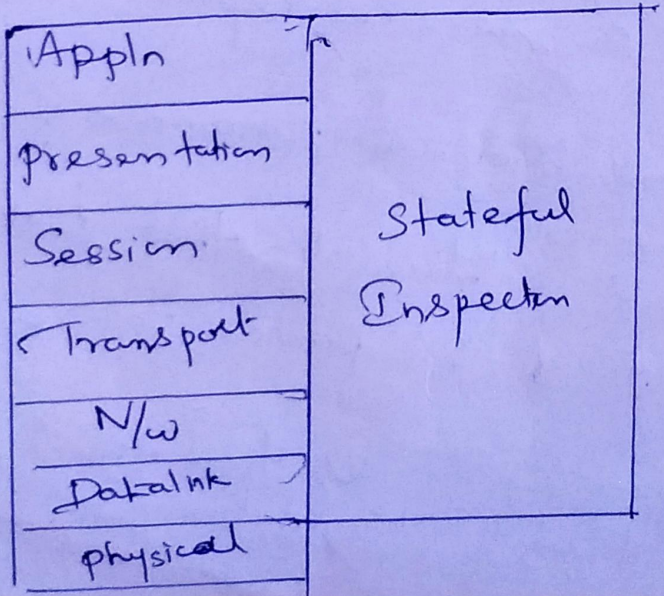
Appln – state ~~Route~~ table

Transport → Accen table

Network → Access Rules

Inspection module





advantages

→ One pkt filter can protect an entire n/w

→ Efficient

→ Supported by most routers

Disadvantages

Difficult to Configure Correctly

Difficult to test Completely

2) Application gateways:

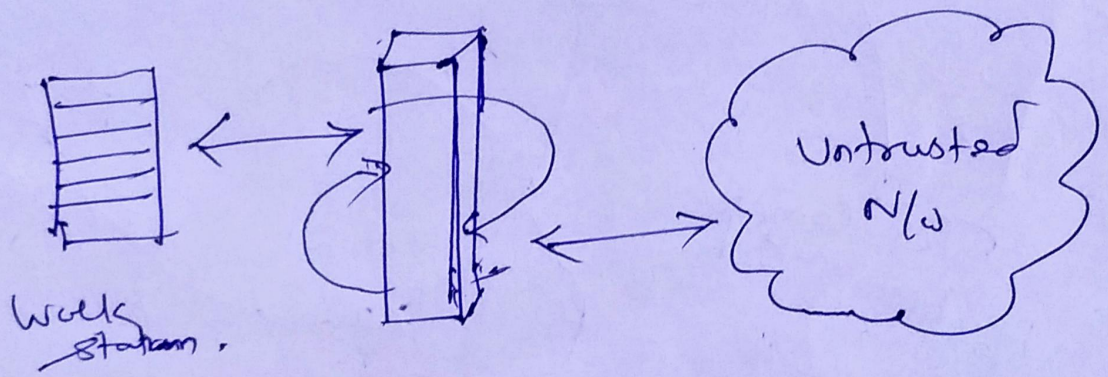
It is also known as proxy Server Since it runs Special s/w that acts as a proxy for a service request.

→ One Common example of proxy Server is a Firewall that blocks (or) requests for & responses to request for Web pages & Services from the internal Computers of an organization.

→ appln fire walls work at the application layer

→ The interaction is controlled at the appln layer.

→ With the proxy acting as mediator, the source & destination systems never actually connect.



4) Circuit gateways:

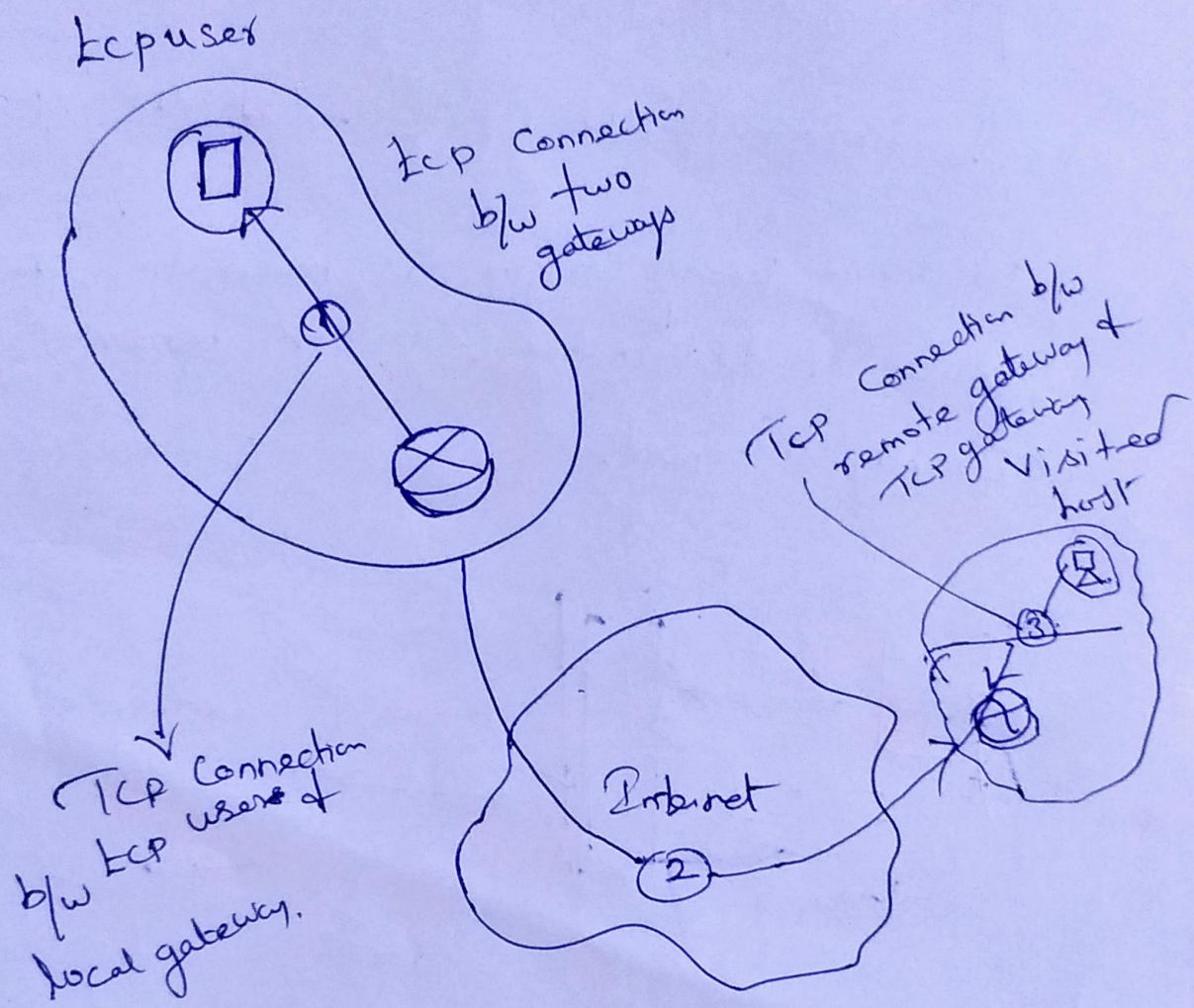
→ Operates at the transport layer

→ relays two TCP connections (Session layer)

→ Monitor handshaking b/w packets to decide whether the traffic is legitimate.

→ Socks commonly used for this

Circuit Level firewalls examples.



MAC Layer firewalls:

Design to operate at the media access Control layer

→ using this MAC addresses of Specific host Computers are linked to ACL entries that identify the Specific type of packets.

5) Hybrid Firewall:

Combined the elements of Other types of Firewalls.

ex: packet filters + proxy services

Types of Firewalls

Stateful Firewall
Stateless Firewall.

Stateful Firewall is able to hold in memory Significant attributes each Connection from start to finish.

It may include the following details

IP addresses
Ports &
Sequence numbers of the packets.

Stateless firewall:

Treats each n/w packt / frame in isolation.

→ It is trying to establish a new Connecten

ex FTP → File transfer protocol.

Advantages of firewall:

→ Stop incomy calls to insecure Servers
→ Control accen to other services.
→ Control the Spread of Viruses
→ Cost effective

Disadvantages of firewall

→ Cannot prevent insider attacks
→ Smuggling
→ Bottleneck for performance
→ Doesnot protect the back door.
→ Restrict legitimate use of the Internet

11 Intrusion Detection System:

→ Intrusion : type of attack on information assets in which

→ Intrusion detection Consists of procedures & Systems Created & Operated to detect System intrusions

Intrusion Detection System (IDS):

→ Detects a violation of its Configuration activation alarm.

→ Many ID's enable administrators to Configure systems to notify them directly of trouble via email (or) pagers.

IDS terminology:

* Alert / Alarm
* False negative: The failure of an IDS system to react to an actual attack event.

False but show not false.

→ false positive:

false but shows not true.

An alarm/alert indicates that an attack is in progress (or) that attack has succesfully occured when in fact there was no such attack.

→ Confidence value

→ Alarm filtering.

IDS classification

It has two detection methods

(i) Signature based

(ii) Statistical anomaly-based.

IDS operate as

→ N/w based

→ host based

→ application based

→ Signature based:

It is widely used because many attacks have clear & distinct signatures.

Statical Anomaly-Based IDS

It is used to compare the traffic that is known to be normal.

→ When measured activity is outside baseline parameters - IDS will trigger an alert.

→ IDS can detect new types of attacks.

→ It may generate many false positives

N/w based IDS: (NIDS).

It Resides on Computer (or) appliance Connected to Segment of an organization's n/w looks for signs of attacks.

→ It is installed at specific place in the n/w where it can watch traffic going into & out of particular n/w Segment.

Advantage:

It can enable organization to use a few devices to monitor large n/w

disadvantage:

→ It Cannot analyze encrypted packets.
→ It Cannot reliably ascertain if attack was Succesful or not

Host based IDS:

It resides on a particular Computer / Server & monitors activity only on that system

→ Benchmark & monitor the Statues of key System files & detect when intruder Creates, modifies (or) deletes files.

Advantage

It can Detect local events on host System. & detect attacks that may elude a n/w based IDS.

disadvantage:

It can use large amounts of disk space

Application based IDs

It examines appln. for abnormal events.

Application IDs may be configured to intercept requests

→ File System

→ N/w

→ Configuration

→ Execution Space.

Advantage

It can observe interaction b/w application & user.

Disadvantage:

More susceptible to attack

Spoofing.

IDS Control Strategy

(1) Centralized

(2) Fully distributed

(3) Partially distributed

Centralized:

All IDS Control f/n/s are implemented & managed in a Central location.

Fully Distributed:

All Control f/n/s are applied at the physical location of each IDS Component.

Partially Distributed:

It Combines the two. Centralized & ~~Fully Distributed~~ while individual agents Can still analyze & respond to local threats

Honey pots

Decoy Systems designed to lure potential attackers away from critical Systems & encourage attacks against themselves.

Honey Nets:

Collection of Honey pots Connecting Several honey pot Systems on a Subnet

Padded Cell:

Honey pot that has been protected So it Cannot be easily Compromised

Trap & trace Systems

It detects intrusion & trace back to its source.

Usually it consists of honey pot (or) padded Cell & alarm.

Legal drawbacks to trap & trace:

* Enticement → is legal & ethical.
* Entrapment → is not legal & ethical.

III Scanning & Analysis tools

Attack protocol is series of steps/processes used by an attacker in a logical sequence to launch attack against a target system or n/w

Foot printing:

Internet addresses collected during foot printing.

Finger Printing:

It reveals useful information about internal structure & operational nature of target system/n/w for anticipated attack.

Tools:

(1) **Port Scanners:**

Tools used by both attackers & defenders to identify computers

active on a n/w & other useful information

(ii) Firewall analysis tools.

This is used to discover the Firewall rules & administrator in analysing the tool.

It helps to minise the risk from an attack.

→ Packet Sniffers:

It collects Copies of packets from n/w & analyses them.

In the wrong hands Sniffers can be used to eavesdrop on n/w traffic

→ Wireless Security tools:

Security professional must assess risk of wireless n/ws.

Wireless Security toolkit should include the ability of to Snift wireless traffic, Scan wireless hosts & assess level of privacy & Confidentiality afforded on the wireless n/w.

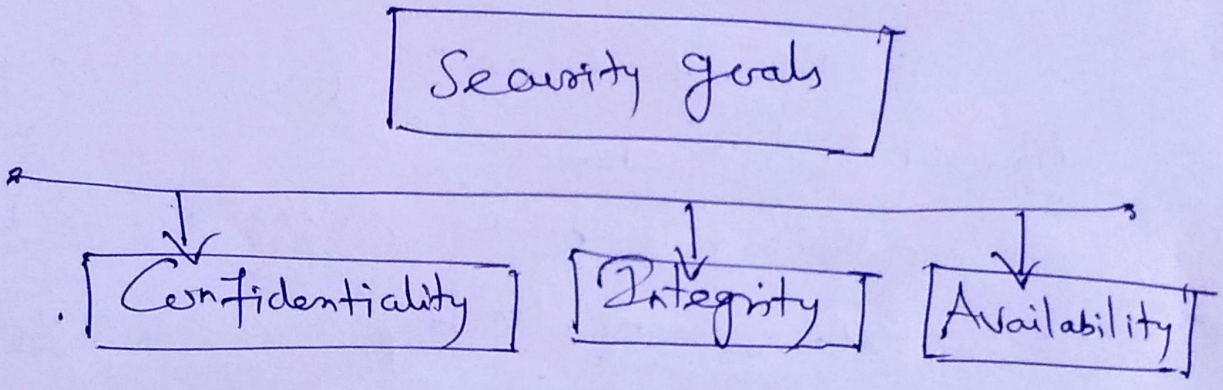
IV Cryptography:

Security goals:

There are three Security goals

→ Confidentiality
→ Integrity
→ Availability.

Taxonomy of Security goals:



Confidentiality

Keeping information secret from Unauthorized users/access.

Integrity

Information needs to be changed Constantly. ex. In a bank. When a customer

deposits (or) withdraws money, the balance of their accounts needs to be changed.

Integrity means that changes should be done only by authorized users & through authorized mechanisms.

Availability

The third Components of Security is availability. The information Created & stored by an organization needs to be available to authorized users & applications. Information is useless if it is not available.

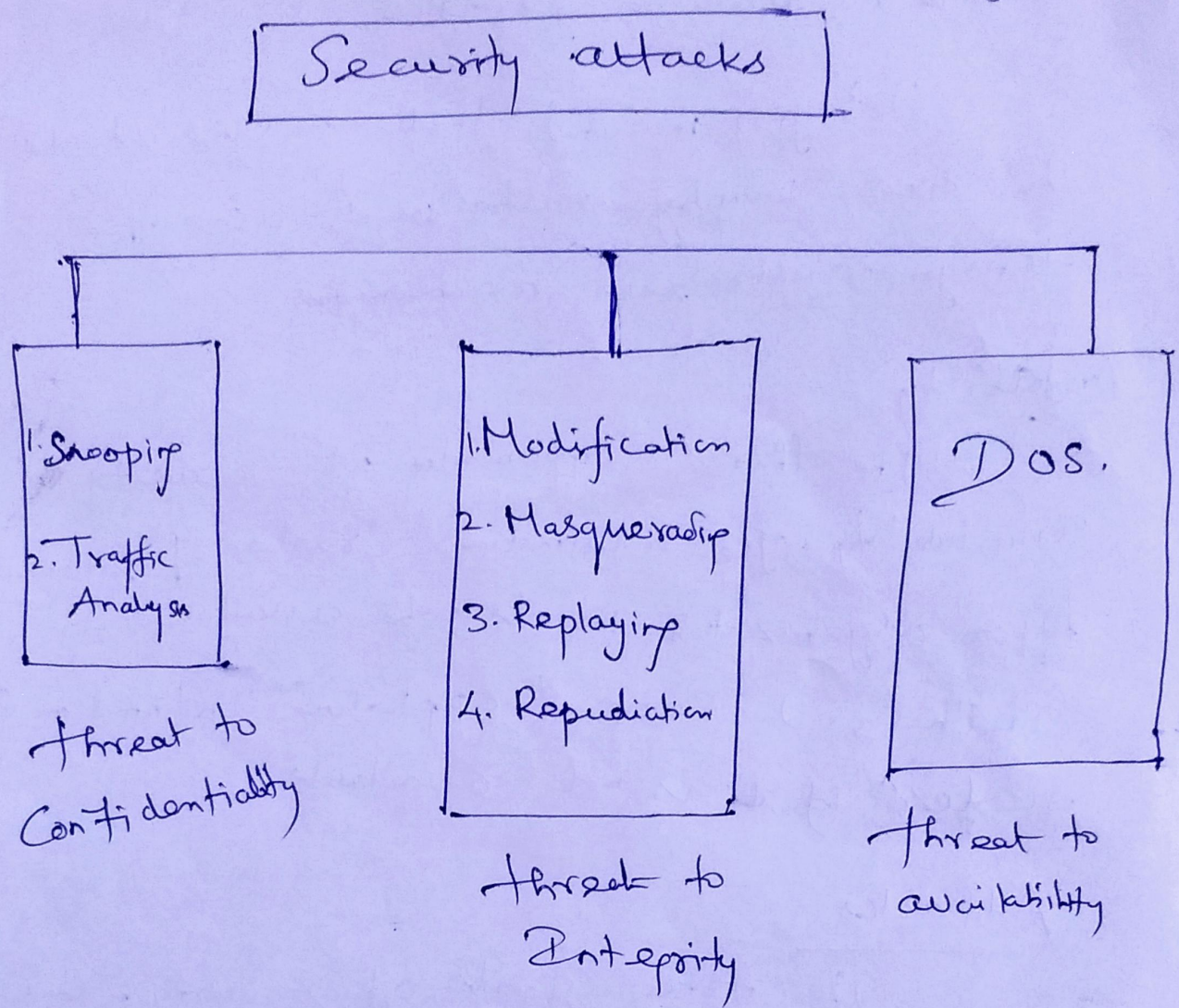
Attacks:

The three goals of Security - Confidentiality integrity & Availability - can be threatened by Security attacks.

: It has three Security attacks.

threat to Confidentiality, threat to integrity & threat to availability.

taxonomy of attacks with relation to Security goals.



Security Services

→ Data Confidentiality
→ Data Integrity
→ Authentication
→ Non repudiation
→ Access Control.

Techniques

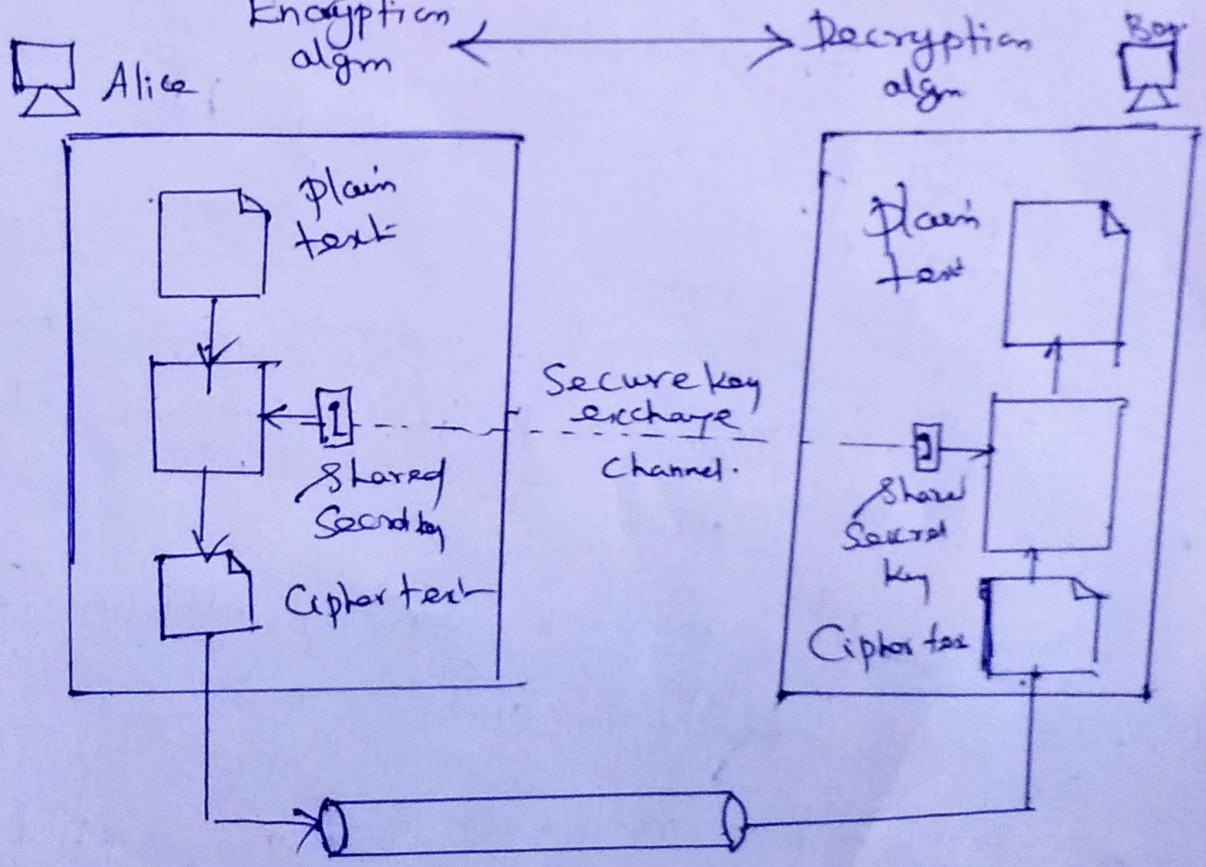
Two techniques are prevalent today

(1) Cryptography means → Secret writing

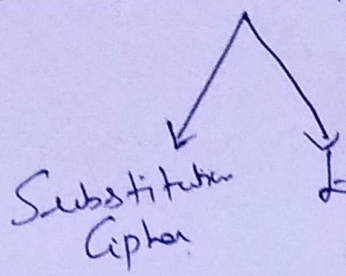
(2) Steganography means → Covered writing (or Secret writing)

Symmetric key Cryptography:

The general idea of Symmetric-key Cryptography



Traditional Ciphers.



Substitution Cipher

replaces one symbol with another.

Ex

If the symbols in a plain text are alphabetic characters, we replace characters with another

Cipher key is encrypted as the message "hello"

Transposition

It doesn't substitute one symbol for another instead it changes the location of the symbol.

Ex message Enemy attacks tonight.

add one bogus character 'Z'.

enemy attac kston ightZ.

Modern Symmetric key Ciphers.

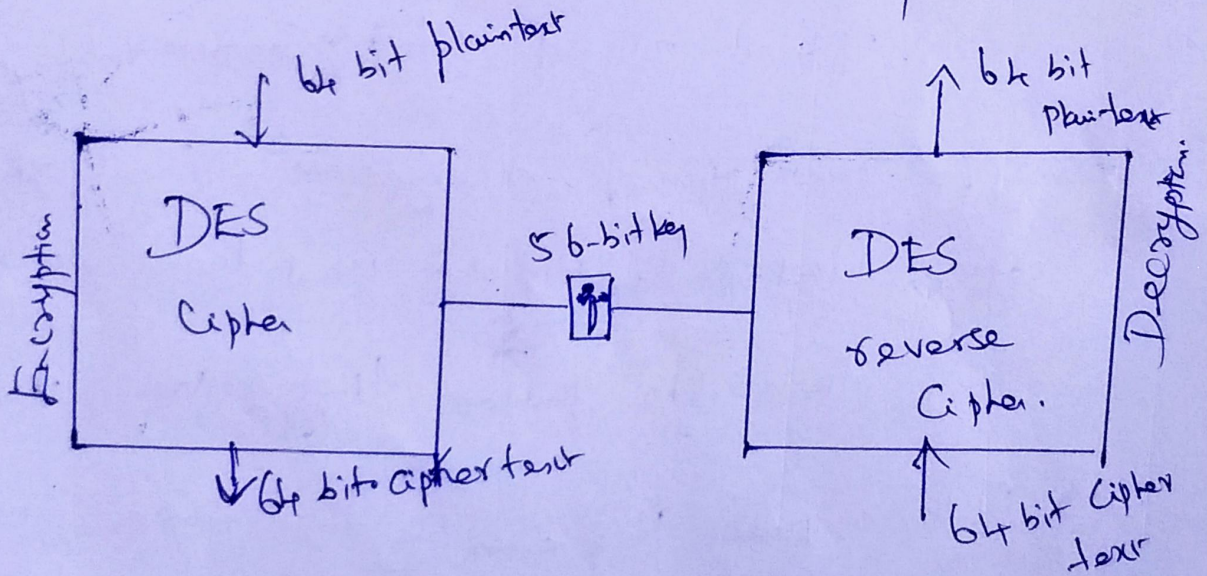
There are two modern Symmetric key cipher.

(i) DES

(ii) AES

1) DES : . Data encryption Standard is a Symmetric Keycipher.

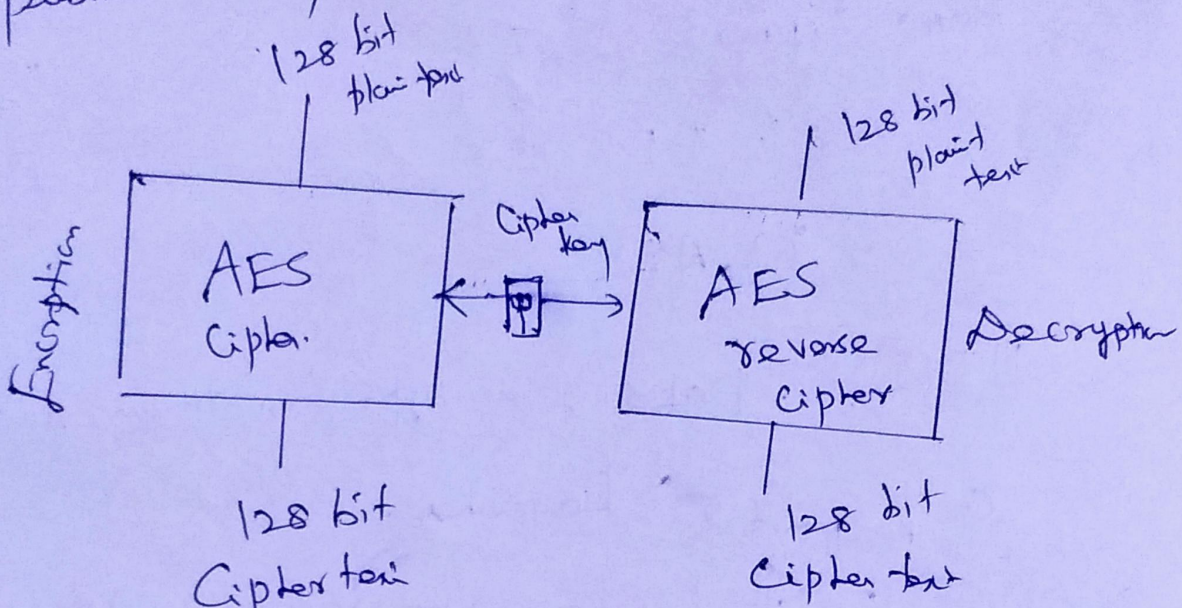
It has been the most widely used Symmetric-key block Cipher. Since its publication



This figure depicts the general design of the DES Encryption Cipher.

AES:

It is Advanced Encryption Standard published by NIST



Asymmetric key Cryptography

It is used for Confidentiality

If encryption & decryptions are thought of as locking & Unlocking pad locks with keys, keys then the padlock that is locked with a public key can be Unlocked only with the Corresponding private key. & draw the appropriate diagram for the assymetric key Cryptography.

V Access Control devices.

Successful access Control System includes no. of Components, depending on System's needs for authentication & authorization

Authentication:

It is validation of a Supplicant's identity

Four general ways in which authentication is Carried out.

- What Supplicant knows
- What a Supplicant has
- Who a Supplicant is
- What a Supplicant produces.

Authorization

Are you allowed to do that).

Once you have access. What can you do?.

Enforces limits on actions.

Authentication

How to authenticate a human to a m/c ?

Can be based on

→ Something you know

- for ex ; a pwd

→ Something you have

- for example, a smart card

→ Something you are.

- for example ; your finger print

* pwds

* Lots of things act as passwords !

— PIN
— Social Security number
— Mother's maiden name
— Date of birth
— Name of your pet , etc.

Trouble with passwords.

passwords are one of the biggest practical pbms facing Security engineers today.

Why passwords?

✓ Cost : passwords are free

✓ Convenience: easier for SA to reset pwd than to issue user a new thumb.

Keys Vs passwords

Crypto Keys:

✓ Spse key is 64 bits

Then 2^{64} keys

Choose key at random

Then attacker must try about 2^{63} keys.

Passwords

* Spse pwds are 8 characters &
256 diff. characters

↳ 2^{64} pwds $= 256^8$

↳ Users do not Select pwds at random.

↳ Attacker has for less than 2^{63} pwds to try. (dictionary attack)

Good & Bad pwds

Bad pwds

4444

pickachu

102560

frank

Good pwds:

POkeomN

OnceuPonALImS

JJ1ej,43j-EmmL+y

password Experiment

Three gps of users → each gp

advised to select pwds as follows

Group A : At least 6 char · 1 non-letter

Group B : Password based on passphrase.

Group C : 8 random characters.

* Results

Group A : About 30% of pwds easy to crack

Group B = About 10% cracked

• passwords easy to remember.

Group C : about 10% cracked.

• passwords hard to remember.

Attacks on pwd:

Attacker could

Target one particular account

Target any account on System

Target any account on any System.

Attempt DoS attack.

password Retry

How long should it lock

- 5 seconds
- 5 mints
- Until SA restore source

passwd file

Bad idea to store pwd in a file.

But need a way to verify password.

Cryptography Solution: hash the pwds

Store $y = h(\text{password})$

password Cracking:

Attack1 pwd without dictionary

- Must try $2^{56}/2 = 2^{55}$ on average.

expected work is about

- $\frac{1}{4}(2^{19}) + \frac{3}{4}(2^{55}) = 2^{54.66}$.

→ Attack any of 1024 pwds in file.

→ With dictionary

probability at least one pwd is in dictionary is $1 - (3/4)^{1024} = 1$

If Salt is used

↳ Without dictionary expected work is 2^{55}

→ Assume 2^{10} pwds are distinct.

→ Need 2^{55} comparisions before expect to find pwd

→ If no salt we can precompute all dictionary hashes & amortize the work.

→ pwd Cracking is too easy.

Biometrics

Biometric seen as desirable replacement for pwds Ex fingerprint
Hand written signature
facial & speech recognition

Biometrics modes:

- Identification → what goes there
  ↳ Compare one to many
  Ex FBI fingerprint db.
- Authentication: Compare one to one
  Ex Thumb print.

VI Physical Security:

Physical Security is as important as logical Security.

Seven major Sources of physical loss

* Extreme Temperature
* Gases
* Liquids
* Living organisms
* Projectiles
* Movement

Physical Access Controls.

(i) Controls for protecting ~~the~~ Secure facility.

* Walls, Fencing & gates
* Guards
* Locks & keys
* Dogs
* ID Card & badges.
* Mantraps
* Electronic Monitoring
* Alarms & alarm Systems.

* Computer room & wiring closets
* Interior walls & doors.

(ii) ID Cards & badges:

- Ties physical Security with Information access Control
- Serve as single form of biometrics (facial recognition)

(iii) Locks & keys:

Two types of locks
mechanical & electromechanical.

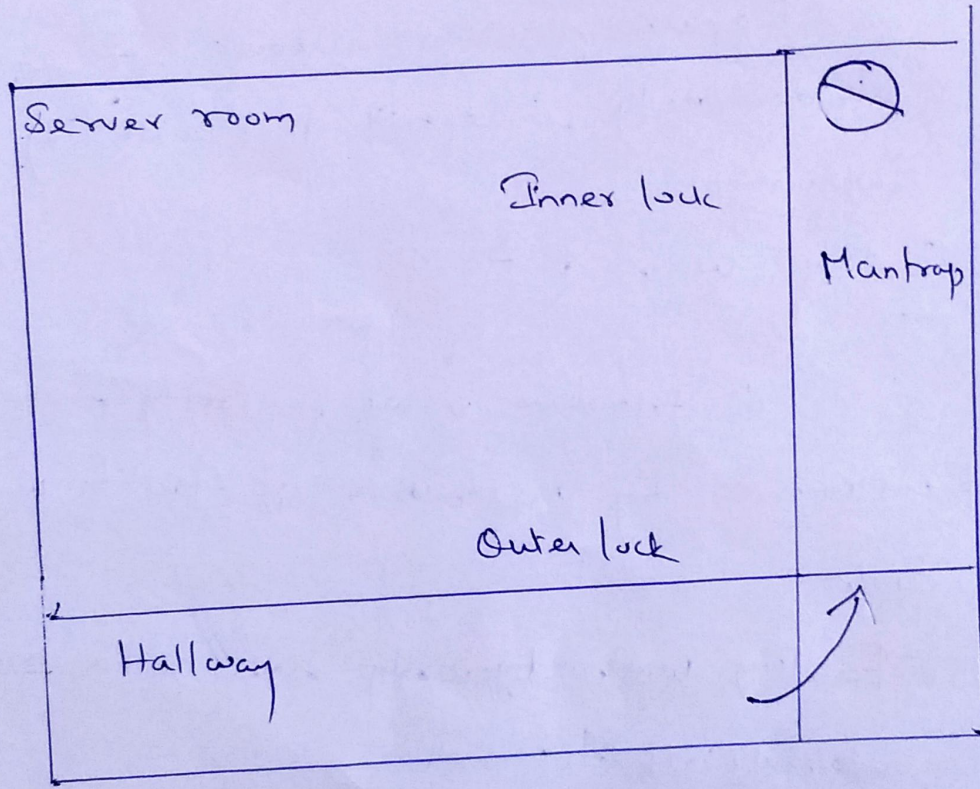
* Locks can also be divided into four categories
  * Manual
  * Programmable
  * electronic
  * Biometric
* Locks fail & alternative procedures for control access must be put in place.
* Locks fail in one of two ways.
  - Fail-Safe Lock
  - Fail Secure Lock.

Mantraps.

Small enclosure that has entry point & different exit point

Individual enters mantrap, requests access and if verified

→ Individual denied entry is not allowed to exit until security official overrides semantic locks of the enclosure.



5) Electronic monitoring.

Records events where other types of physical controls are impractical / incomplete.

Drawbacks.

Reactive : do not prevent access / prohibited activity.

Alarm & Alarm Systems.

Defined fire, intrusion, environmental disturbance, or an interruption in services.

6) Computer rooms & wiring closets

Require special attention to ensure Confidentiality, integrity & availability of Information

7) Interior walls & Doors:

Information asset security sometimes Compromised by construction of facility walls & doors

Facility walls typically either standards interior (or) Firewall

8) Fire Security & Safety:

Most Serious threat to safety of People who work in an organization is possibly of fire

9) Fire Detection & Response:

Fire Suppression Systems:

Devices installed & maintained to detect & respond to a fire

→ Deny - an environment of heat, fuel or oxygen.

10) Fire Detection:

Fire detection systems falls into two general categories

* Manual
* automatic.

there are three basic types of fire detection systems.

* Thermal detection
* Smoke detection
* flame detection.

11) Fire Suppression

→ System Consists of portable, manual or automatic apparatus.

→ portable extinguishers are rated related by the types of fires

Class A, Class B, Class C & Class D.

III Power Mgmt & Conditioning:

Electrical quantity is a concern, as is quality of power.

→ overloading a Circuit causes problems with Circuit tripping & can overload electrical Cable increasing risk of fire.

IV Inventory mgmt:

& Computing equipment should be inventoried & inspected on a regular basis

* physical Security of Computing equipment data storage media & classified documents Varies for each organization.

VII Security of Personnel:

Employees often feel threatened When organization is creating/enhancing overall information Security Pgm.

* positioning & Staffing the Security fn/-.

The Security fn/- Can be placed within

* IT fn/-
* physical Security fn/-

Administrative Service fn/-

Insurance & risk mgmt fn/-

Legal department

Organizations needs to enforcement with needs for education training, awarness & Customer Service

Staffing the Information Security fn/..

→ Selecting personnal is based on many criteria including Supply & demand.

→ Many professionals enter Security market by gaining skills, experience & Credentials.

Qualifications & Requirements.

The following factors must be addressed.

Mgmt Should learn more about position requirements & qualifications

⇒ Upper mgmt should learn about budgetary needs of Information Security fn/..

→ organizations typically looking technically qualified Information Security professionals who Understand

Organization look for most mainstream IT technologies.

→ Threats facing an organization & how they can become attacks

→ Entry into the Information Security profession

→ Today, students select & take degree pgm to prepare for work in Information Security.

Information Security position:

→ Chief Information Security officer (CISO or CSO)

Top information Security position frequently reports to chief information officer.

Chief information Security officer.

Develop information Security ~~prog~~ budgets

Security Manager:

→ Accomplish objectives as identified by CISO

Employment Policies & practices.

Employement Policy & Practices

1. Termination
2. When employee leaves organizations.

- There are a number of security related issues Employee Collects all belongings.

→ Friendly departures include resignation, retirement promotion (or) relocation.

→ Official information used by the employee must be inventoried files stored or destroyed & property returned to organizational stores.

→ If information has been copied (or) stolen action should be declared an incident & the appropriate policy followed.
