→ Threats, Attacks & their types

Threat: A threat can be anything that can take advantage of a vulnerability breach security & negatively alter, erase, harm object or object of interest.

Security thread: It is defined as a ~~security~~ risk that which can potentially harm computer system or organization.

→ Types of Security threads:

i) Trojan Horse
ii) Viruses & worms
iii) Spy ware
iv) malware
v) Back doors
vi) Cookies
vii) Key logging
~~viii) DOS attack~~

→ malware :

→ malware is not a virus, In fact it consists of viruses, worms, trojan horses, adware etc..

→ In simple words it is a code with intent to steals data or destroy something on PC

→ Viruses :

→ A computer virus is a carefully hidden piece of computer code that has the ability to spread from one system to another

→ It replicates & executes itself usually doing damage to your computer in process.

→ Worm:

→ It is a self replication program that can spread through out a network without human assistance.

→ Worms Causes damage similar to viruses, stealing info, courupting files, installing backdoor for remote access etc.., (huge memory & bandwidth is used.)

→ during File sharing, email attachments these are shared.

→ Trojan horses:

→ It is a destructive program, usually pretends a computer game/application.

→ if exauted, computer system will be damaged.

→ usually comes with monitoring tools.

→ It doesnot have the abidity to self replicate but to deliver destructive payloads & unlike ~~unload~~ viruses, worms.

→ Spy ware:

→ It is a program that gets installed without users permission

→ It moniters the users activity on the internet & transmit that information to the third party.

→ Root kits:

→ It is a simple/single program or a collection of program designed to take complete control of system.

→ It gives hackers all the abidity of system administrator from a remote location.

→ Back doors:

→ Back doors trojan allows some one to take control of another users computer via the internet without their permissions.

→ Cookies:

→ These are files on your computer that enable websites to remember you details

→ Track your visit

→ It can be threat to confidentiality, but no to your data

→ Key dogging:

→ It is the process of ~~security~~ secretly recording key strokes by an unauthorized third party.

→ For stealing username, passwords credit card details etc...

→ Attacks: it is gaining the access of data by unauthorized user.

→ gaining can be accessing data, modifying data & destorying data

Attacks

Passive attack

→ Here only data is accessed by the attacker.

→ No modification of data done here

→ low damage

ex: The release of message content, Traffic analysis

Active attack

→ Here both data can be accessed & modified by the attacker.

→ modification can be done

→ high damage

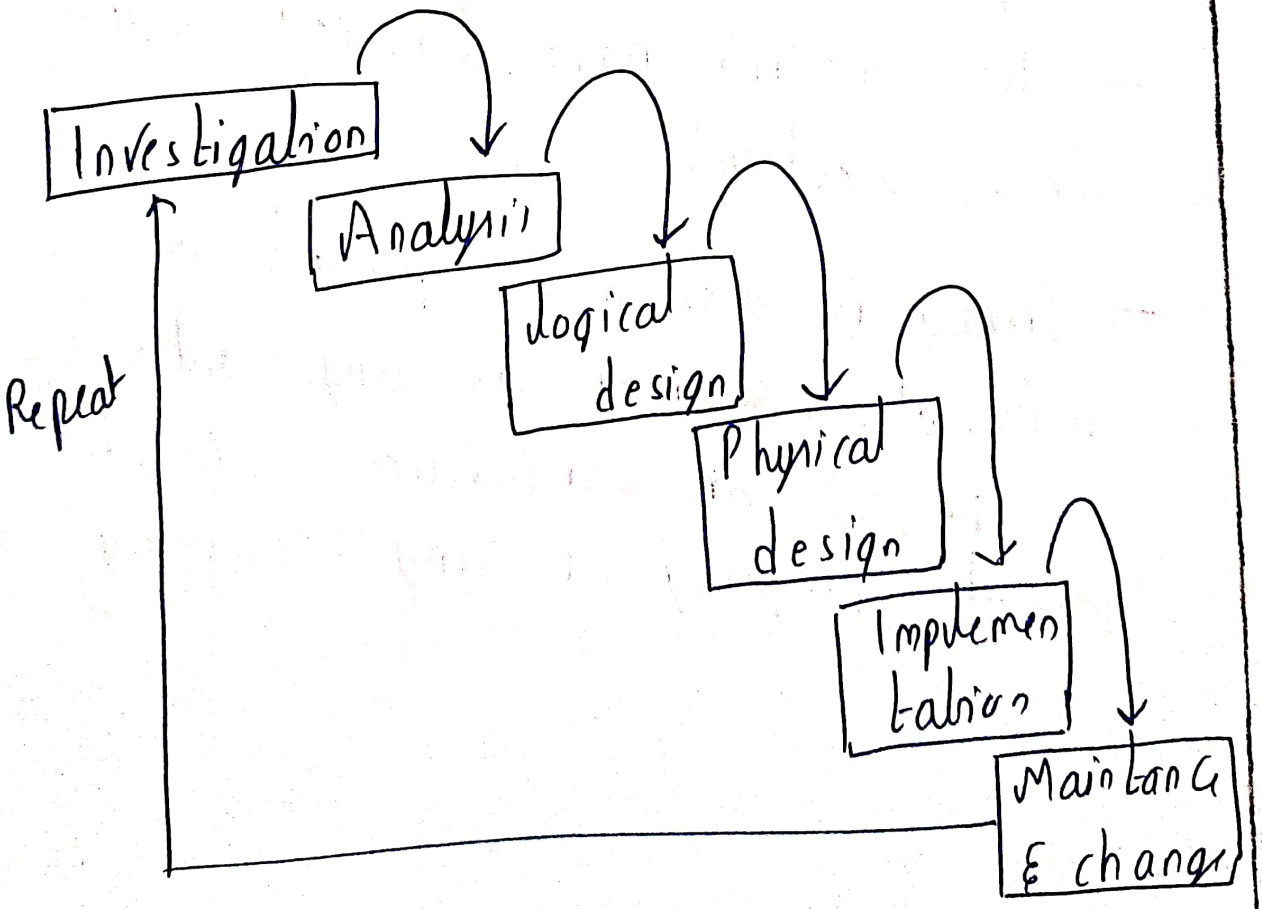
ex: Masquerade, Modification of message, Repudiation, Replay, Denial of servic

→ Secure System Development life cycle:

→ The same phases used in traditional SDLC may be adapted to support specialized implementation of an Information security projects.

→ Here the identification of specific threads and creating controls to counter them.

→ in short form it is called SecSDLC.



System Investigation :- (what it can potentially do)

→ This process is started by officials/directives working at the top level management in organization.

→ the main goal is to know what problem is the system being developed to solve.

→ all the objectives, constraints & scope of project are specified

System Analysis :- (understanding system properties checking for threats)

→ In this phase detailed document analysis of the document from the system. Investigation phase are done

→ Previously existing security policies, applications & software are analysed in order to check faults & vulnerabilities in the system.

Logical Design: (planning for idea which could solve threats)

→ Main In the logical design phase, the information from the analysis phase is used to begin creating the solution.

→ The main goal here is to make a logical blueprint that involves all the requirements

Physical Design: (designing a blueprint).

→ The technical team acquires the tools & blueprint & start implementing the software & by applying the security aspects (new).

Implementation: (Final product of software is made here. with testing).

→ here the final product or software is made or purchased

→ all the main stages like ordering, receiving testing are done here.

→ here an aggressive testing is done here & Final system documentation are written

Maintenance:

→ This is once of the longest & most expensive phase

→ after the implementation of the security program it must be insured that it is Functioning properly & managed according.

→ Frequently this process is repeatedly for the better security.

→ When any kind of bugs or threats reported again the whole process starts & the issues are resolved

→ Secure SDLC is nothing but SDLC with security (from threats).