Computer Security

Security is the freedom from theft

Computer security is not limited to hardware. Computer security has to do with the protection of the computer hardware information & data contained in it.

Who are the people involved?

- The experts: Who studies computer security to prevent theft
- The users/owners of the computers
- perpetraters.

- There are two classes of perpetrators: insider & outsider
  * overt
  * covert
  * unintended.

- insider overt: This is a threat sponsored by disgruntled employees for the purpose of destroying data & equipment.

- Insider covert: This is a form of threat

Breaked for the purpose of criminal intention.

- Unintended insider attack: This type of attack occurs as a result of human error and neglect of duties

- outsider overt: This involves physical attack on the computer network or other network facility

- Outsider covert This has to do with attack from rogue softwares sent from personal computers to the company's computers
- Outsider unintended: it has to do with the attack on the outside which is not intended

There are three classes of computer security:

1. Physical security
2. Rogue Software
3. Network security

Why do we need Security?

① Computers Lack Intelligence

It is true that modern science and technology have led to the invention of sophisticated computers that are very fast, accurate and very powerful in the computing and manupulation of data. but these computers are not efficient in performing tasks that require Intelligence. Lack of intelligence exposes computers to security threats which compromise integrity of the system.

② The ease of Compromise

The Integrity of a computer can be easily broken because of its many weaknesses. A perpetrator ~~may need to find~~ only needs to find one of the weaknesses in other to do harm.

③ Simpliaty of the Operating System

A computer is designed to be controlled by an operating system. Operating system by nature are ~~extremely~~ complex. For ease of usage, A system programmer would have to design an operating system such that it is less complex which makes it less secure.

(9) Connection to the Internet and its Protocols.

Communication is one of the benefits resulting from the use of the internet. For communication to be possible, the computers require to have a communication standard, which results in the development of communication protocols. This protocol is a set of rules that specifies the individual steps of a complete internet session. For computers to be able to send, forward & receive mails they must execute the same protocols. These internet protocols have been developed many years ago before the internet security became a serious issue. Which is why the security features included in the protocols are usually weak.

The ten(10) laws of Security

1. If someone can persuade you to run his program on your computer, it is not your computer anymore.

2. If someone can alter the operating system on your computer, it is not your computer anymore.

3. If someone has unrestricted physical access to your computer, it is not your computer anymore.

4. If you allow someone to upload programs to your website, it is not your website anymore.

5. Weak password defeats strong security.

6. A computer is only as secure as its owner/user is trustworthy.

7. Encrypted data is only as secure as the decryption key.

8. An outdated antivirus scanner is only marginally better than none at all.

9. Absolute ~~abnormity~~ anonymity isn't practical in real life or on the ~~web~~.

10. Technology is not a panacea.

① Disaster recovery

② Recovery requirement, policy, strategy, execution of recovery plans, document & backup system

③ Loss estimation, developing secure computer systems, external security measures, issues, security models

④ Discretionary access requirements, mandatory access requirements, user authentication, access & information flow control, auditing & intrusion detection, damage control & assessment, microcomputer security, entropy, perfect security, unicity distance, complexity theory, NP-Completeness, Number theory, cryographic system, public system, Digital signatures, Network & telecommunication security, fundamentals objectives & threats, distributed system security, trusted network, firewalls

ERR. OMOSIGHO

DISASTER RECOVERY & PLANNING

Disaster recovery and planning is an important part of any organization.

Disaster recovery & planning is the detailed steps required to quickly RESTORE TECHNICAL CAPABILITIES & SERVICES after a disruption or disaster has occured. The idea in such a plan is to minimize the impact that a catastrophic event will have on the organization

Aspect of organization under Threat,
① operation ② Reputation ③ Confidence
④ Human & capital resource.

* expand on the four points above & more on Discover recovery & Planning
* Don't end your definition without four points above

Disaster Recovery Requirements

① Threat Analysis
② Disaster criteria
③ Cost of deprivation
④ Additional networking requirements

The sole goal of ~~dis~~ the customer disaster recovery plan is to ~~give~~ keep the customer in ~~peo~~ business with minimum disruption in the event of a major disaster.

Recovering from Disaster

① First line of defense, is to minimize the possibility of disaster occurring. Steps must be taken to protect people, data and facilities from natural & man-made disaster.

② The next step is to make provisions for system backup.

③ Targeted Systems can be moved into a seperate center to continue operation

④ Create set of policies, procedures, facilities and services designed to address minimal operation

⑤ Physical security = ~~access control~~, This includes access control, prevention and

protection of network facilities

(6) Emergency procedures:- We have documentation, training (pertaining to handling emergency situations).

(7) Diagnosis- Procedures for determining the cost; Find out what led to the incident; forecast the extent of damage, proceed with a remedy, offsite storage system,

(8) Recovery Centres:- Providing facilities for backup of the system.

(9) Manpower Availability & Testing:- ~~Availability~~ of manpower, Additional manpower

Under testing we have periodic testing of various aspects of the recovery plan.

CYBERSECURITY => EGGR. PRUDENCE

Four classes of physical attack

① Invasive: This physical attack has to do with depackaging of the chip in order to get direct access to its inside components

② Non Invasire: This employs externally available information such as the power consumption or timing

③ Active: Tries to tamper with the device's proper funation for instance a fault induction attack that induces error into the data.

④ Passive: Observes the system behavior while it is running without any disruption. The essence is to mimic the system and create a similar one with same error.

The Side Channel Attack

It is a form of attack based on obtaining information from the implementation of a computer system while disregarding the weaknesses in the implementation of the implemented algorithm.

* How to obtain the spied information through timing, power consumption, electro magnetic induction or sound.
  - running time
  - Power consumption.
  - Electromagnetic radiation
  - Sound produced from keyboard perharps

Physical Threats to the computer

① Power surge

Use UPS or Power surge protector

② Threat to the physical security of the computer - Theft

Use controlled access, burglary proof doors, card operated doors, security cameras

③ Attack on the magnetic field: the hard disk can be affected if not protected

properly.

④ Static electricity in the body

Try to discharge the static electricity from the body before opening the computer.

Physical Protection of Data:

① Store in the hard disk, flash drive or cloud

② Have a hard copy

⑤ Spying: A computer system being monitored without the consent of the owner, to have access to unauthorized information. Protect your system against spywares.

⑥ Data Integrity: Strings of bits being altered.

ENGR. PRUDENCE

VIRUSES

- Operating Systems are sets of routines that supply services to the user in order to make it easy to use

Services provided by Operating system *

① Helps to boot computer

NB: How does a virus operate?

NB. Characteristics of Comp. Virus

Assignment

① Discuss the historical development of Virus

② Discuss briefly the factors that will cause a person to become a virus writer

Virus Propagation

Virus propagation can be from a file to another file in the same computer. It can also be from one computer to another computer. There are different ways this can be achieved:

① Through executable files

NB: During propagation, ensures that it doesn't do multiple infestation because the aim is for it to be hidden, so if it does multiple infestation, it will really increase/decrease the file, thereby making the owner notice that something has gone wrong.

② Through the memory
③ Through infested software
④ through file sharing
⑤ Through email

VIRUS CLASSIFICATION

~~Virus can~~ Virus can be classified as follows:

① By the Infection mechanism of the virus
② By the damage the virus inflicts
③ By the trigger mechanism
④ By the platform or operating system the virus infests.

Infection Mechanism of the Virus

This form of infection can be a Boot sector infestor, file sector infestor, email virus, macro virus

Classes of file Infestor

① Shell Virus - forms a shell around the original file/program

② Non-overwriting Virus - It embeds itself inside the infested program & erase a part of the program

③ Intrusive Virus - It replaces some of the orginal code of the program, particularly the part responsible for handling interrupt

④ Simple Virus - Most times, it is introduced into the computer as part of the host program

Boot Sector Infestor

Macro virus - It infests itself in a data file

Operating System Virus: It copies itself into one or more of the operating system

General application virus - attaches itself to an application & gets executed each time an application runs on a system.

Virus Life Cycle

The lifecycle of a virus is made up of 3 stages

① activation ② Replication ③ Operation

* Read the remaining up.

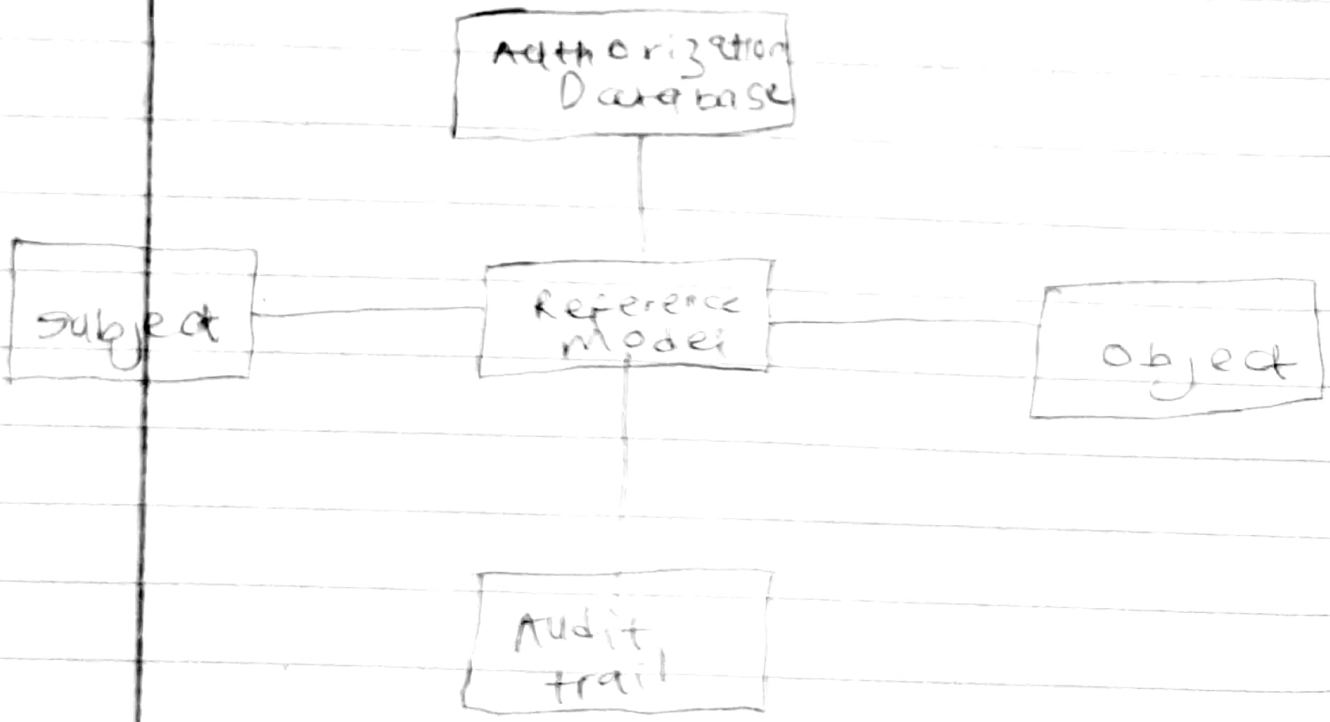
EXAM: CDIA

COMPUTER SECURITY => A

What is an access control policy (find out)

Access control is a method of guaranteeing that users are who they say they are and they have appropraite access to ar organization's data. It has two main funationing:

① Authentication ② Authorization.



Subject - System users or group of users

Object - files, printers, scanners, etc.

Audit trail - log of all those who have accessed, time of access, etc

Authorization Database - Indicates the rules that allow subjects to interact with objects and the reference model applies that to the situation.

Reference model - Contains the operations and the rules that determine whether the subject is able to access the object and how they are able to do that.

There are three basic access control models:

① Discretionary access control (DAC) model

This model is based on the

* Find out other access control

discretion of the data owner or creator

② Mandatory Access control (MAC)

It is a model in which people are granted access based on an information clearance. What that means is that access rights are assigned based on regulations from a central authority. Most times, authority comes from the administrators of the Operating system.

Different levels of Information Access in an Organization.

① Unclassified ② Confidential ② Secret

③ Top Secret

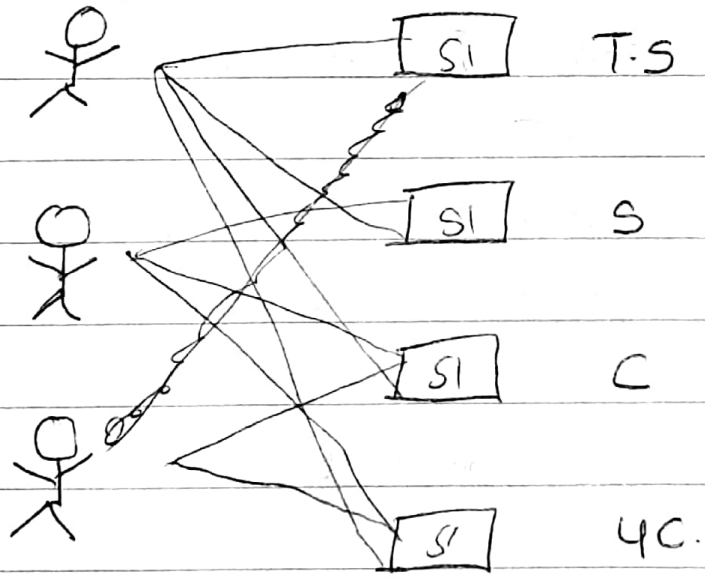
Top secret ↑ * You cannot read up but you can read down if you have a need-to-know

Secret

Confidential

Unclassified low to high.

* Top secret cannot read information meant for levels below it. (It can only write. If needs a token to do so. need-to-know
* Anybody can read unclassified



Other models

Role-based reference model, ~~Attribute~~ Attribute based reference model, rule-based reference model.

technologies that support access control models

Access control list, Access control matrix, constrained user interface, content dependent access control, context dependent access control

Assignment

1. Adv & Disadv of DAC & MAC
2. Discuss the role based model.
   (Meaning, adv & disadv, you could do a comparative disadv & adv
3. Discuss the attribute based model.
4. Discuss the importance of access control
   (in less than 1 or 2 pages, soft copy)

* Submit by thursday 00:01 am.

font size 10

GODE. SYLVESTER

CPE 515

- NON-TECHNICAL ATTACK
- ~~Dialogue~~ Dial up network
- V~~irtual~~ (Virtual) private network
- I~~ASTRU~~ Intrusion detection access control
- Scanning and analysis tools
- Port Scanner

Assignment

① Discuss the historical development of Virus

ENGR. PRUDENCE

Worms

A worm is a software program that is executed INDEPENDENT of other programs

Worms have the ability to replicate itself and spread from one computer to another.

NB: Worms dwell on the vulnerability of a program to operate.

A worm propagates from host to host by exploiting a security hole or vulnerability discovered by its creator.

The key feature of a worm is that it has the ability to propagate very fast.

Worm Propagation Techniques

1. Hit list scanning
2. Permutation scanning
3. Topological scanning

Hit List Scanning

Worm, by nature, has low initial rate of infection. A well designed worm can overcome this low initial rate of

→ for it to be able to propagate fast, it requires a certain num

through the use of the Hit List Scanning

For the Hit List Scanning, the hacker begins by preparing a list of IP numbers (btw 10,000 to 50,000) for computers on the Internet having good internet connection. Once that list is ready, the hacker builds the list of IP numbers into the worm, the worm is then released into one of the computers on the hit list; and then the worm starts scanning the list inside the computer in order to probe the computer to look out for weaknesses in order to harm the computer. When a vulnerable host is found, it prepares to infest it. It does that by dividing the list in two. By dividing the list in two, it sends a copy of itself to the computer with one half of the list and keeps the other half. As new copies of the worms spread throughout the internet, they carry shutter lists. When a worm is generated with a list, of say, L it switches from the hit list mode to it's

normal mode of scanning and propagation. The hit list, assists the worm to achieve deep initial penetration of the internet in a very short period of time. Studies shows that using hit list, worms can infest millions of computers in a few seconds.

Permutation Scanning (PS)

NB: i) One disadvantage of hit list is that it is possible to have IP numbers generated more than once. PS helps to curb this.

ii) With hit list, it is difficult to measure its success so as to estimate the level of worm penetration. PS helps to curb this.

The permutation scanning is designed to solve two problems:

i) Generating of IP numbers more than once.
ii) Measuring the level of penetration of

the coorm.

Permutation scanning depends on the worm's ability to find out whether a potential target has already been inpected. The Permutation scan requires the worm to generate all the IP numbers but in this case the numbers are not generated in their natural form. The coorm then generates a permutation of the IP numbers. These permutations are generated using an encryption algorithm. The coorm then has to implement such encryption algorithm. It uses a key to encrypt each 32-bit IP number to another 32 bit number. The same key can be used to decrypt it when necessary. When the algorithm is applied to encrypt all the IP numbers in their natural order, the result is a sequence of the same numbers but in a different order which is the permutation.

Permutation scanning helps the coorm

coordinate their effort and enables the worm to determine the extent of its success in terms of worm infection.

Topological Scanning

This approach works with local information found in the computer. Once the worm exhausts the local information (list of email addresses, url locations, etc) it will switch to permutation scanning.

NB: Worms cannot achieve deep penetration if there is no internet.

Worm Communication.

When a worm creates a copy of itself it sends that copy of itself, with its IP number to a known location so that the originating worm becomes a parent while the destination worm becomes the child. If the destination worm sends a copy of itself, it attaches the IP number and the IP number of its parent; in order

to generate a forward communication between the nodes. The problem with backward communication is that the child worm is likely not to going to be able to communicate with its parent.

Ways in which we can Control Computer Security Threats

1. Quickly identify any outbreak.
2. Isolate, disassemble & ~~disco~~ understand the newly discovered threat.
3. Actively fight new infections
4. Anticipate new types of viruses and worms and educate the computer security community about these future threats
5. Plan methods and tools to detect the anticipated threats
6. Educate the public about computer security and safe ways of using the computer.

Prevention & Defense Against Rogue Software Attacks

① Understand the vulnerability that worms and viruses exploit and try as much as possible to minimize their propagation.

Examples of vulnerability

① User sympathy : It cannot happen to me

② Insuppicient security control : Lack of hardware and software programs for detection

③ Misuse of available security features.

④ Weakness in the operating system.

⑤ Unauthorized User

⑥ Abnormity of networks

Defenses Against Worms & Viruses could involve!

① Technical means

② Common Sense in using the computer

③ Legal means

Next class! Antivirus software.

Anti-virus Software.

An anti-virus is a program or set of programs designed to prevent, search for, detect and remove software ~~programs~~ viruses as well as other malicious softwares like worms and trojans, ~~etc~~.

~~for example, ne~~

Types of ~~Anti~~ virus Software

1. Virus-Specific
2. Generic
3. Preventive techniques.

Virus-Specific: Looks out for viruses and identifies them.

How it operates

It searches or scans files in the disk or in a particular directory. It is looking for bit strings that signals the presence of viruses. Once located, the software gives the user the choice to either delete the virus automatically or place the infected file in quarantine for detailed inspection on a later time

or it outrightly ignores it.

Generic Virus Detection

It examines the files on the disk or programs in memory for anything suspicious, unusual or abnormal.

NB: This technique cannot identify the presence of a specific or known virus but it can warn the user about any suspicious thing that has taken place or about to take place in a particular file or in a particular memory resident program.

Preventive Techniques

It creates an atmosphere where viruses, worms, trojans, etc cannot thrive ~~strive~~

This creates an environment in the computer where viruses cannot thrive once they have gained access into it.

In summary, an anti-virus software is expected to perform the following tasks

so as to uphold the integrity of the computer!

(i) Detect all known viruses & malware already located in the computer, advice the user on each occurrence once discovered and assist the user in deleting them.

(ii) Detect unknown viruses.

(iii) Scan incoming mails, all downloaded files and any removable storage device inserted into the computer so as to detect all known viruses and rogue softwares in them.

(iv) Keep record of all its activities in a log file.

Firewall

This is a combination of hardware & software for the purpose of deciding which kind of request and what type of data packet can pass to and fro from a computer or local network. Firewalls for a personal computer is normally fully implemented by software while those for a small network of computers employed at

home are implemented using a hardware firewall that is built into the router. The major task of the firewall is to block certain requests of data transfer based on the rules built into it to ensure decision making.

A typical firewall begins with some built-in rules which the user can read to, delete from or even modify. The firewall enforces access policy through the built-in rules which decides what data packet property to be examined and whether to let the packet through it or not.

A firewall can perform the following tasks:

1) Limit incoming data so that data coming from certain senders will be blocked

2) Limit outgoing data so that a program is not able to send data out without the knowledge of the owner.

NB: Firewall rules can be simple or complex

3) Generates and saves a log of all its activity especially on data packet it has blocked.

4) Perform all its task fast and transparently to its user.

NB: A complex firewall ~~the~~ rule checks several conditions while the simple rules checks only a single condition.

Components of a Firewall

The main components of a firewall are:

1) Gate 2) Choke

The Gate is responsible for the transfer of data and also blocks data from going out.

The choke serves as a filter that decides which data to be blocked.

Features of the firewall

1) For content filtering

② Bandwidth management
③ Bandwidth Accounting
④ Connectivity Logging.

CPE 515 - ENGR OPIA

Security Models

Bell - Lapadula

The Bell - lapadula model is a confidentiality model that is concerned with keeping sensitive data secure. In this model, security/sensitivity levels are used for subjects while clearances are used for objects

In this model, all objects must be labeled from the most sensitive (top-secret) to the least sensitive (Unclassified or public).

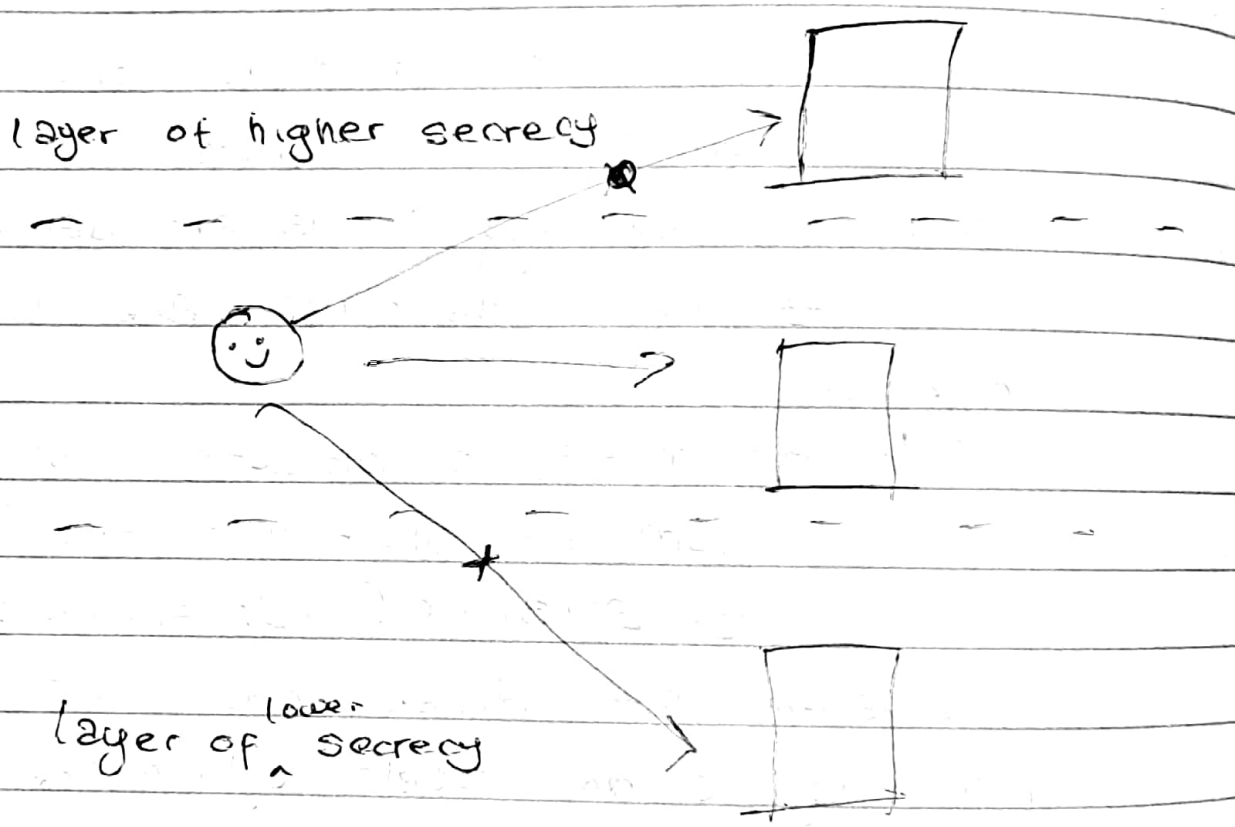
Systems are divided into users which are subjects and labels which are objects i.e All objects must have a label for the system to work properly. This is considered a state machine with a set of allowable system state, thus preserving the security of information even as the system moves from one state to another.

Properties of the model

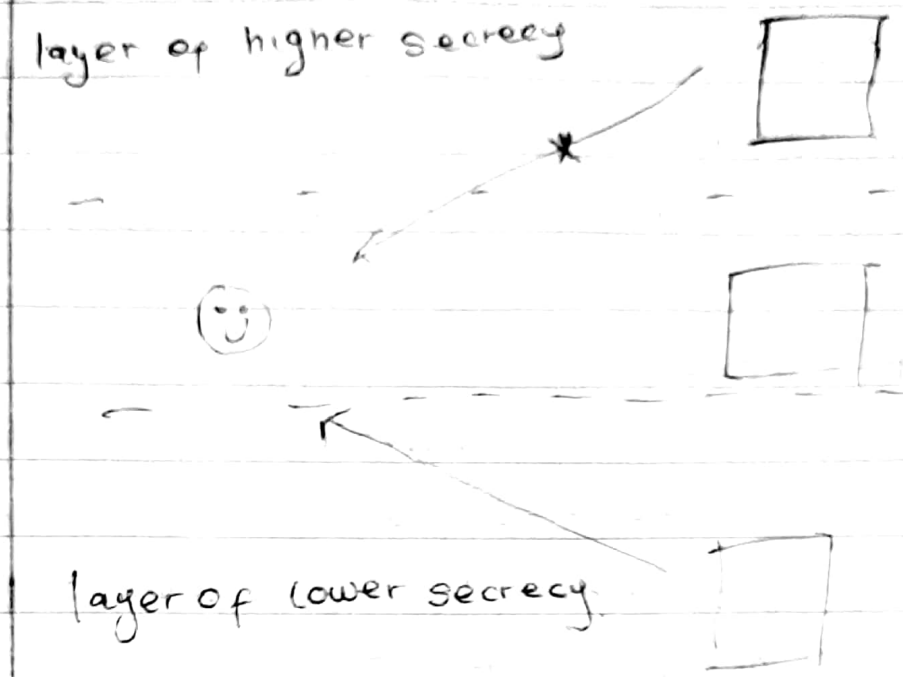
(1) Star property (No write down, NWD)

It prevents subjects with high level

data clearance from writing information to objects of low data clearance.

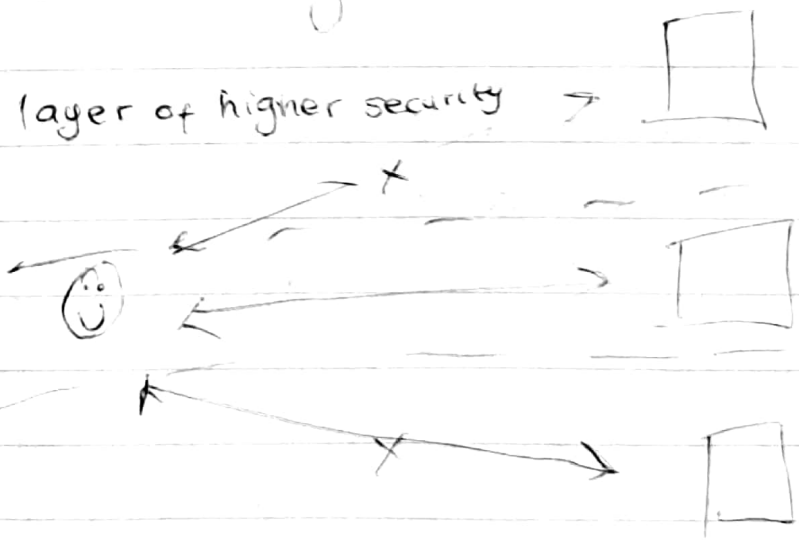


2) Simple Security Property (no read up)
The user cannot write to the lower level as what he/she writes might contain sensitive data.



(3) Strong Star Property

You can only read & write for your own level. You cannot read and write for lower or higher level.



(4) It uses an access matrix of subjects and labeled objects to determine which subjects are permitted to access each object

Biba Model

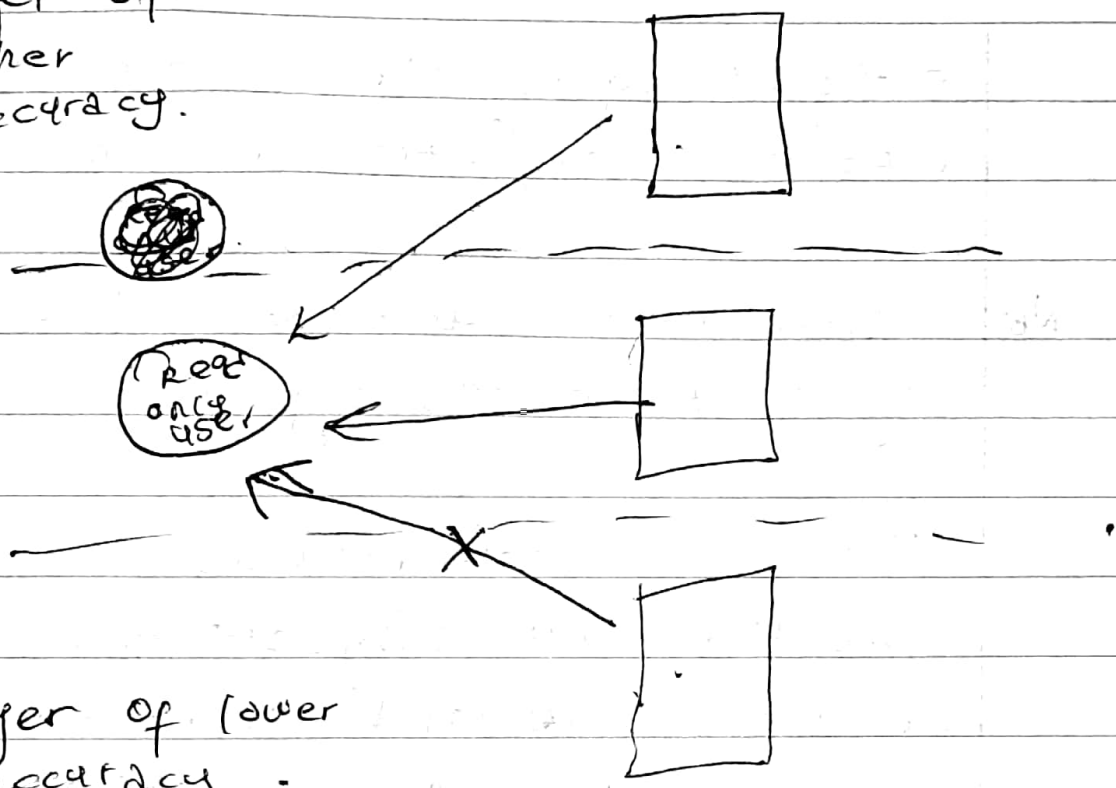
Concerned with data integrity so that data is not modified without authorization. In the Biba model, Integrity levels are used instead of sensitivity/security level. These rules will prohibit users from making inappropriate modification ~~authorization~~ of data & prevent the corruption of data caused by introducing Unreliable information. This model uses the MAC & the Lattice Model.

Properties

① No Write up and No read down

The subject cannot read object of lesser integrity or trust levels and subjects are not permitted to write data from a layer of low integrity or trust to a layer of higher integrity or trust.

layer of higher accuracy.



layer of lower accuracy.

* Find out strong star property for Biba model.

② Invocation Property

This means that the users cannot request any service from an object with a higher Integrity level

Access

This is the flow of information between the subject & the object. It

is the ability of the subject to perform a task or an interaction with an object.

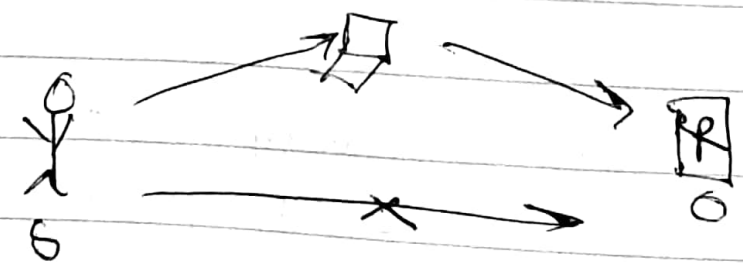
NB: Subject: users at different levels
Object: Resources e.g files.

There are some models that make sure that the subjects and objects are acceptable and are based on a defined security policy. These models are:

1. State machine model
2. Lattice-based model.
3. Non-interference model
4. Information flow model.

State machine model

* Clark Wilson Model.



* Look up internal & external security