Module - IV

Protection, security & OS case Studies

=> protection	security
* A method used in OS that manages threats within the systm to maintain the proper ()-ing of the systm	- - - - that handles threats frm outside of the sytm to maintain - - - - - - -
* control the access to the systm resources	provide the systm access to legitimate users only.
* Handles quite simple queries	Handles more complx concerns
* Focuses on internal threats of the systm	focuses on ex threats to the systm.
* more convoluted queries are handled	Simple queries are handled.
* Encryption & ~~a~~ authentication mechanisms are used	authorization mechanisms & implemented.

=> Protection :

* refers to mechanism for controlling the access of prgms

* used -

policy → security & mechanism → protection (pro)

~~pro~~

to provide a mechanism for enforcemnt of the policies.
to improve relialeility by detecting hidden errors.
to ensure that each prgm component active in a systm

* protection mechanism —

Access control matrix:

- It is a security model of (pro) state in comp systm. It is repsnted as mtrix.
- Access matrix is used to define the right of each (p) executing in the domain with respect to each obj.
- An access mtrix can be imagined as a □-lar array of cells, with 1 row per subject & 1 col^n per obj.

	FileA	FileB	printer
Alice	Read, w	R w	print
Bob	R w	R w	p
chris	R		p
david		R	
guest			

fig: A.C. mtrix.

* can be implemnted in 3 ways —

breach → [illegible].

① Global table, ② Access list for obj & ③ capability lists for subj

⇒ security prbms:

* A system is said to be secure it its resources are used & accessed as intended under all circumstnces.

* It is easier to protect against accidental misuse than against malicious misuse.

* Attackrs use several standard methods in their attempts to breach security. The most common is masquerading - in which 1 participnt in a commn^n pretnds to be someone else.

* To protect systm, security measures must be implemnted at 4 levels,

1) Physical: The sites containing the comp systm must be physically secured against entry by intruders ([illegible]) This layr is designed to prevnt unathorized physical access to the facility.

2) Network: This layr is designed to protect against ntwrk based attacks & prevnt unauthorized access to ntwrk.

3) Application : 3rd layr of Security. includes measures like Secure coding practices, penetraⁿ testing. This layr is designed to protect against appliⁿ level attacks like SQL injection.

4) OS : OS must be kept upto date & configured & modified to use the attack surface & avoid penetraⁿ.

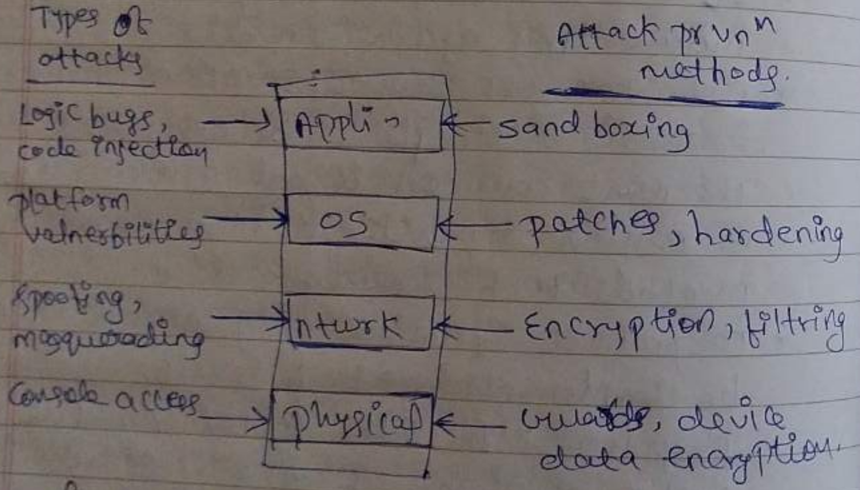
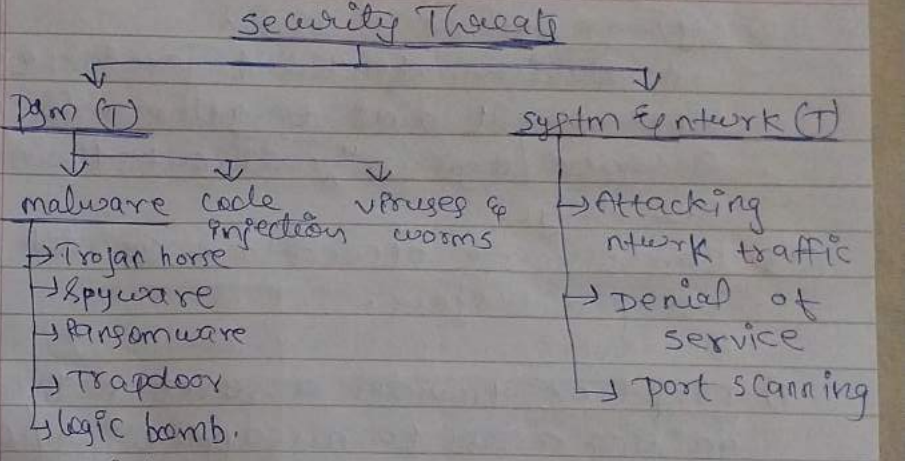


fig : 4-layered model of security.

=> major Security threats :

A systm is said to be Secure if its resources are used & accessed as intended under all circumstances.

Security Threats



I Pgm (T) :

OS's processes & kernal do the designated task as instructed. If a user Pgm made these (p) do malicious task, then it's PT

a) Malware :

- It is a malicious s/w designed to cause damage to a comp, srvr, client.
- does ~~not~~ the damage after it is introduced into targets comp.
- malwares —

1) Trojan horse :

It is a type of malware that disguises itself as smthing legitimate bt once installed, can harm yr device / steal info.

2) Spyware :
A variation ~~of~~ on the trojan horse is Spyware. It aims to gathr info about a person / organiz^n sometimes without their knowledge.

3) Ransomware attacks are carried out using a trojan.

4) Trapdoor provides a secret method of gaining access to an appli^n os / online ~~devices~~ Services.

5) Logic bomb : A trap door may be set to operate only under a specific set of logic condi^n → L.b.
Back doors of this type are difficult to detect.

b) Code injection : It is a malicious injection of code into an appli^n, which is then executed by the appli^n.

* ~~B~~ can rslt in data loss / Corruption, lack of accountability.
* Injection sometimes lead to complete host takovr. It can also steal data & authntication control.

* occurs whn an appli^n evaluates code without validating it first.

c) Viruses & worms :

* A Comp virus is a prgm made of malicious code that can propagate itself frm device to device. once the virus attaches itself to a host, they are infected.
* worms are self-replicating type of malware that enter networks by exploiting vulnerbilties, moving quickly frm 1 Comp to anthr.

II System & network (T) :

* Create a situation in which os resources & user files are misused.
* sometimes a it is used to launch a prgm attack & vice versa.
* Common types → port scanning
  → Denial of service (DoS)
  → Attacking ntwrk traffic.

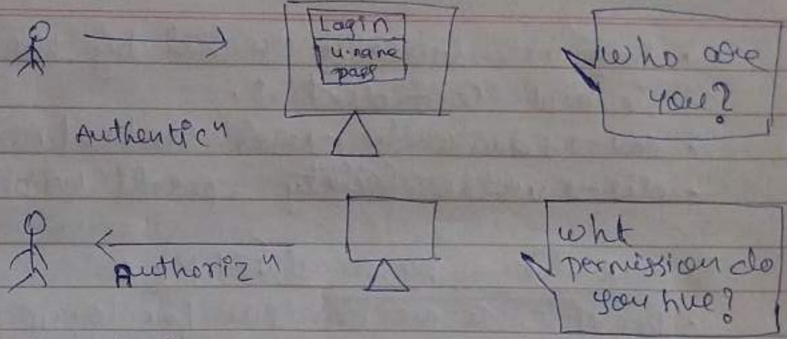
⇒ Cryptography = focuses on ending & decoding data so that it can be interpreted only by the intended recipient.
* Data is trasformed by the use of a cipher / crypto systm (mathematical al)

for encrypting msgs).

* Symmetric crypto^n algo → Secret key crypto^n uses same secret key to encrypt & decrypt a msg.

⇒ User Authentica^n & Authoriza^n =

Authentic^n	Authoriza^n
* Here, identity of users are hacked for providing the access to systm.	Here, user's authorities are checked for accessing the reasources.
* Here, users/persons are verified (confirming the truth of smthing)	Here, users/persons are validated. (ensuring that a (P) / systm meets predetermined req).
* Done bfre authoriz^n (P)	Done after the authentica^n (P)
* It determines whthr the person is user/not	determines 'wht permission does the user hve?'
* Transmit info through an ID token	Transmit info through an access token.



* Authentica^n —

- A user's identity can be determined by —
- wht he is
- wht he has
- wht he knows

* 3 types → Single-Factor (A)
  → 2- " "
  → multi- " "

* commonly used (A) methods for granting access to systm include —

a) passwords :

- It is a method that requires the user to enter their credentials — usrname & passwrd, in ordr to confirm their identity. once the credentials are entered, they are compared against the stored credentials in systm's db & the user is only granted access if the credentials match.

- They are typically created by the user & kept confidential.
- Adv → Familarity, user control.
- dis → vulneralbility, predictability.

b) one-Time password (OTP) :

- provide a mechanism for logging on to a ntwrk using a unique password that can only be used once.
- Are strong (A) providing much better protection to eBanking, coporate ntwrk.
- adv → not vulnerable to replay attacks
- prvnt some forms of identity theft.

c) Biometrics :

- refers to metrics related to humn characteristics
- relies on the unique biological chartrstics of individuals to varify they are who they say they are.

* used to manage access to physical & digital resources like buildings, rooms.

* types → chemical b. devices
→ visual "
→ behavioural "
→ Auditory "

⇒ Mobile OS :

* It is an os that hlps to run othr appli. s/w on mob devices.

* It is the same kind of s/w as the famous comp os like linux & windows.

* eg → symbian os, iphn os, RIM's Blackberry, windows mobile.

* It combines the beauty of comp & hand use devices. It contains a cellular built-in modem & SIM tray for telephony & intrnt connⁿ.

I History :

- pre-1993 — use embedded systms.
- 1993–99 — apple launched newton os, the 1st smartphn — IBM simon.

* palm pilot 1000 personal digital assistnt was introduced with os mob os.

- 2000s — symbian became 1st modern mob os on a smrtphn in 2000.
microsoft's 1st windows CE smrtphns were introduced in 2002.
In 2003, motorola introduced 1st linux based cell phn.
In 2005, Nokia introduced maemo os.
In 2007, apple introduced iphn with ios as ipod.

- 2010s – In 2014, microsoft released windows phn 8.1.
  In 2015, google released Android 5.1 'lollipop'.

II popular mob os :

1) Android os : It is a mob os based on linux kernel & opn-source s/w. Android os was developed by google in 2008.
2) Blackberry os : Developed by Research In motion (RIM). Designed for blkberry handled devices.
   It is benefial for corporate users.
3) ios : developed by apple for the use of its devices. It is the most popular systm tdy. It is very secure os.
   It is not available for any othr mob.
4) Symbian os :
   provide high-level of integran with commun - Based on java lang.
   Developed by Symbian Ltd in 1998.
5) windows : Designed for pocket PC & smrt mob & developed by microsoft.

III Features of mob os :

* M/y mangmnt – It is the managmnt of main / primary M/y. whtevr prg is executed, it has to be prsnt in main M/y.
* processor managmnt –
  whn more than 1 (p) runs on the systm the os decides hw & whn a (p) will use the cpu.
* Device managmnt – Allocates & deallocates devices to diff (p)s, keep rec of devices
* File managmnt – keep rec of the status & loc of files, Allocates & deallocates the resources,
* Security – os keeps the systm & prgms safe & secure through authentican
* data commn – mob phns are now heavily used for data commn like SMS msg, browsing mob websites.
* managing calls – user can manage multiple calls (confrnce calls) & concrnt calls on smart phns.
* Access to intrnt.

⇒ Android OS : (An).

- * (An) is a s/w package & linux based os for mob devices such as tablet comp & smrtphns
- * Developed by Google & latr OHA (opn handset Alliance)
- * Java lang is mainly used to write the (An) code even through othr langs can be used.
- * opn-source, anyone can customize the (An) systm. It provide intresting features like weathr details, opning screen, etc.

* Features —

- • msging – SMS & MMS are available
- • web browsr – based on opn-source Blink.
- • voice-based features
- • Multi-touch, video calling, ex storage
- • Multitasking, screen capture, etc.

* versions —

1.5 → cupcake – soft keyboard

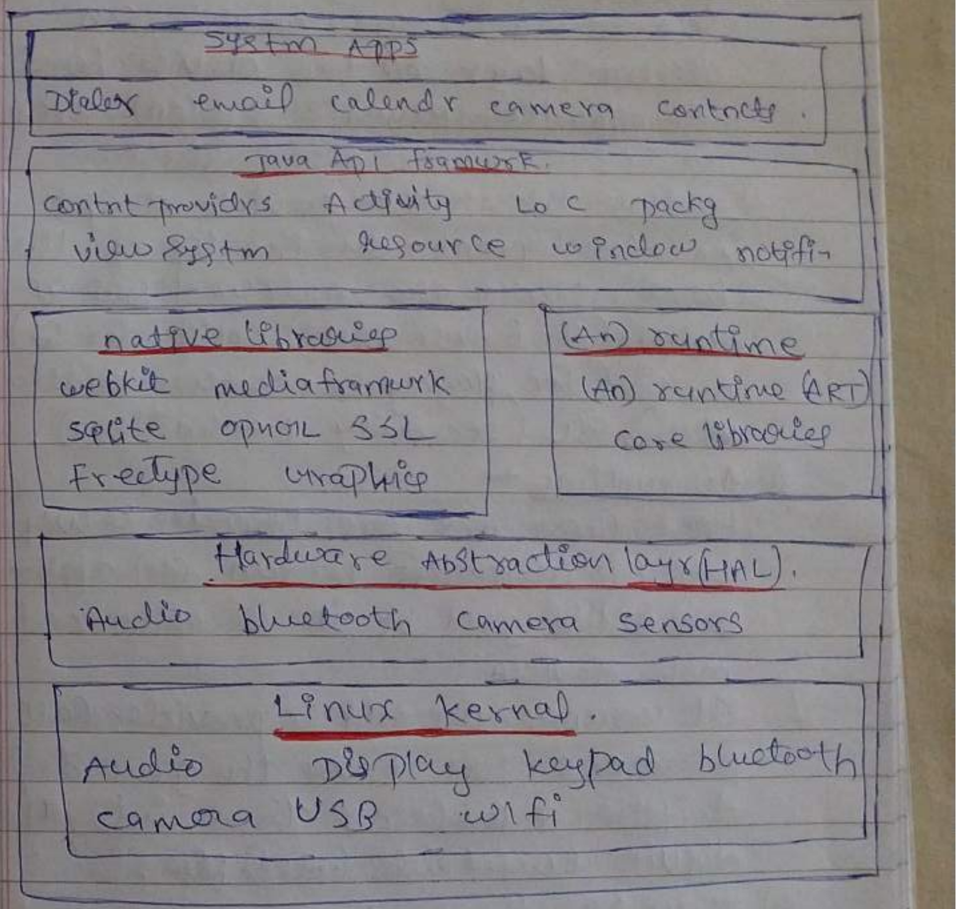
1.6 → donut – advanced search capability.

4.4 → kit kat → more sensors, apps sprt

10 → sprt for foldable phn

11 → new permission control.

I Architecture :



System Apps

Dialer email calendr camera contacts.

Java API framework.

contnt providrs Activity Loc packg view systm resource window notifi-

native libraries

webkit mediaframwrk sqlite opnGL SSL Freetype Graphics

(An) runtime

(An) runtime (ART) Core libraries

Hardware Abstraction layr (HAL).

Audio bluetooth camera sensors

Linux kernal.

Audio Display keypad bluetooth camera USB wifi

1) Linux kernel – It is the heart of (An) archi that exists at the root of an (An) archi –
responsible for device drivrs, power

maugmnt, mly maugmnt, device managmnt & resource access. provide an abstra^{n} layr b/w the device hardware & othr componente of (An) archi~

2) Native libraries – provide a sprt for (An) developmnt. on the top of linux kernel, there are native libraries like — webkit (for browsr sprt), Sqlite (for bd), media (for playing & recording audio & video), SSL (security technology).

3) (An) runtime –
Here there are core libraries & DVM which is responsible to run (An) appli~
DVM is like JVM bt it is optimized for mob devices
It consumes less mly & provides fast prformnce. DVM takes the generated java cls files & combines thm into 1/more dalvik executable (.dex) files.

4) Java API framwrk –
provides the services with the hlp of which we can create particular cls & make that cls hlpful for appli~ creation. Include java API's like ~

provide a lot of clses & interfaces for (An) appli~ developmnt.

5) System Apps –
on the top of (An) frmwrk, there are system apps. (An) comes with a set of core apps for email, SMS msging, calendrs, intrnet browsing~

6) HAL – provides an abstra^{n} layr b/w the underlying physical device hardware & the remaindr of S/w stack.

=) UNIX =

* It is a family of multitasking, multiuser comp OS that derive frm the original AT & T unix.
* Developed by Bell Labs in 1970s
* main concept that unites all the versions of UNIX is follo~ 4 basics –

a) kernel :
kernel of unix is the heart of the os. kernel is the lowst layr of OS & accounts for hardware devices & data storage. It allocates time & mly to prgms, & handle the file str & commu~ b/w keyboard & the screen.

b) Shell :

It is the intrface b/w user & unix kernel, whn a user logs in ~~unix~~unix checks their usname & passwr & then starts a prgm called Shell.

c) cmnds & utilities :

There are various cmnds & utilities which you can make use of in yr day to day activities.

All the cmnds come along with various options.

d) Files & directories :

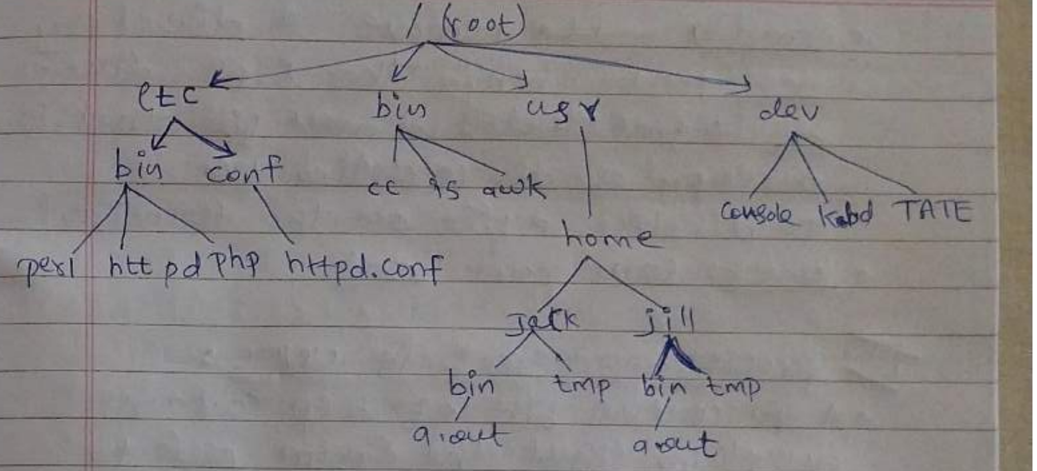
All the data of unix is organized into files. All the files are then organized into directories.

I File manipulation in UNIX :

* A file in unix is a sequence of bytes. files are organized in tree-structured dictories. dictories are files that contains info on hw to find othr files.

* The 1st slash indicates the root of the directory tree → root directory.

* unix directory str —



* A file name '.' in a directory is a hard link to the directory itself.

file name '..' is a hard link to the parent directory.

II user intrface :

* Both prgmr & user of unix systm deal mainly with the set of systms prgms that hve been written & are available for execution. These prgms make the necessary systm calls to sprt their ().

* Common systms prgms can be grped into several categories - most of thm are files / ~~are~~ directory.

eg → mkdir → to create a new directory.

rmdir → to remove a directory

cd → to change the crnt dirn

cp pgm creates a new file that is a copy of an existing file.

To display a file on the terminal, user can run 'cat'

III Process managmnt in UNIX :

* A ⓟ control blk of a ⓟ contains everything that the systm needs to know about a ⓟ.
* virtual add space of a user ⓟ is ÷ into txt (pgm code), data & stack segmnts.
* data & stack segmnts are always in the same add space & usually in oppo dirn. The txt segmnt is sometimes in a add space diff frm the data & stack & is usually read-only.

IV CPU Shedueling in UNIX :

* It is designed to benefit interactive ⓟs, every ⓟ has a sheduling priority associated with it, largr no. indicate lower priority.

* Older unix systm used a 1-sec quantum for the round-robin sheduling. The RR sheduling is accomblished by the timeout mechanism.
* There is no pre-emption of 1 ⓟ by anthr in the kernel.
* ordinary user ⓟs hue the priorities & thus are all less likely to be run than any systm ⓟ.

⇒ Windows NT :

* It is a family of processor - indepndnt, multiprocessing & multi-user OS produced by microsoft.
* 1st version of windows NT is windows NT3.1
* NT is expanded to New Technology
* The design goals that microsoft has stated for NT include extensibility, portability, reliability, compatibility, prformnce & intrnational sprt.

NT provide source-level compatibility to appln that follows the posix standard.

* UNICODE is NT's native char code, although NT sprts ANSI chars by converting them to UNICODE chars bfre manipulating them.

* Architecture —

- HAL (Hardwre Abstra^{n} layr): It is a layr of s/w that hides hardwre diffrnces fr upr levels of the os, to hlp make NT portable.
- kernel: provides the foundation for the executive & the subsystms. It has 4 main responsibilities—
  Thread sheduling, interrupt & exception handling, low-level processor synchroniza^{n} & recovry after a powr failure.
- Executive: provides a set of services that all environmntal subsystm can use.

- environmntal subsystms: Are user-mode (p)s layered ovr the native NT executive services to enable NT to run pgms developed for othr os.

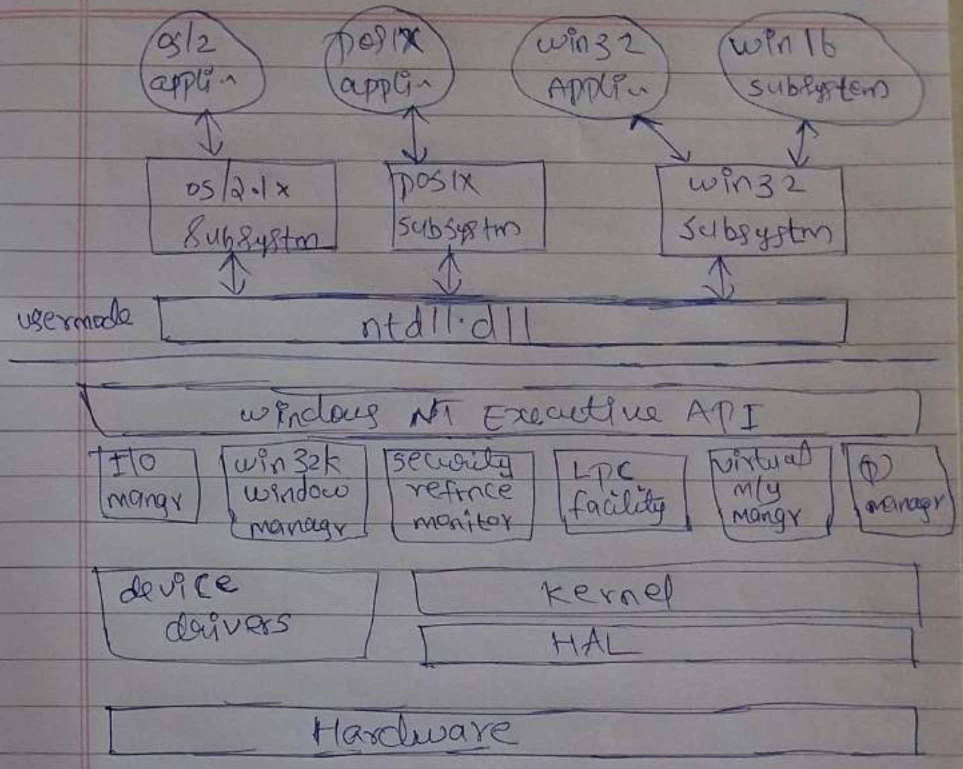


fig : windows NT architecture.