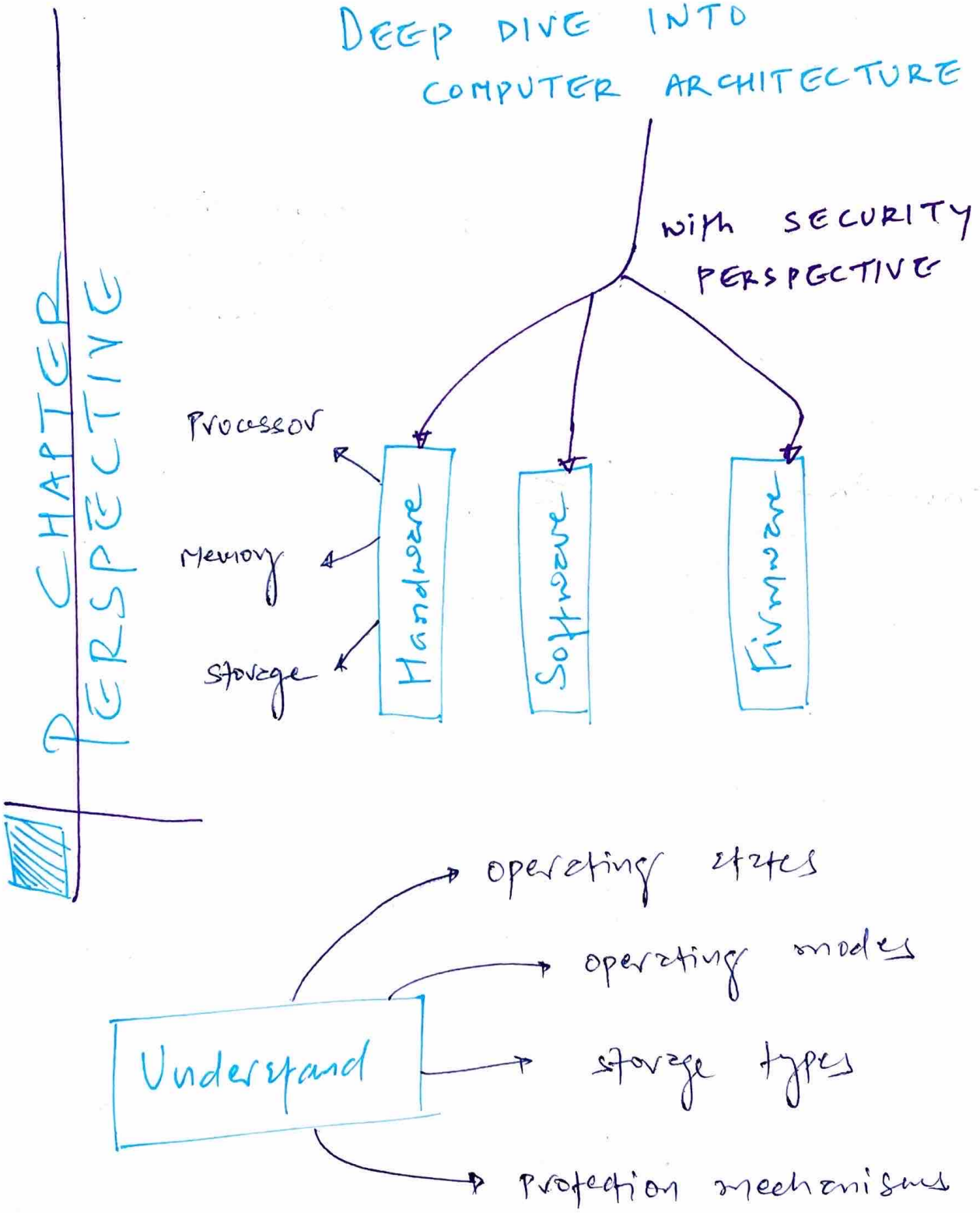
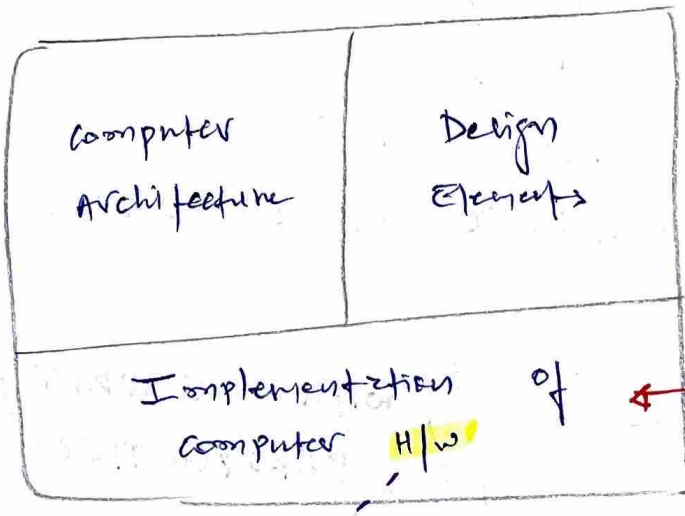
9. Security Vulnerabilities, Threats, and Countermeasures.

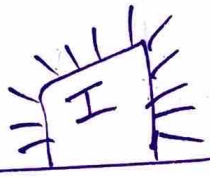


ASSESS & MITIGATE SECURITY VULNERABILITIES



Foundational Understanding of CISSP

HARDWARE



PROCESSOR (CPU)

S/W → OS / Compile

Translate s/w's High-level programming language to Assembly language so, CPU can understand

Computational + Logical operations

Move Demand = Move Power = Advanced Features

→ Execution types (P.T.O)

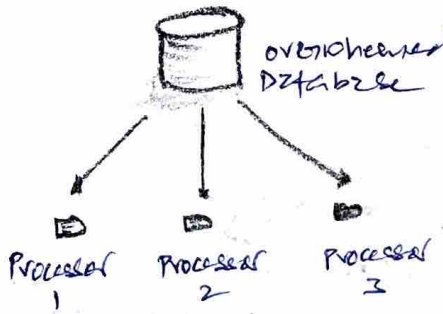
4 Execution Types

Multitasking

Simultaneous execution of one or more task/ application managed by OS.

multiprocessing

More than one processor to increase computing power.

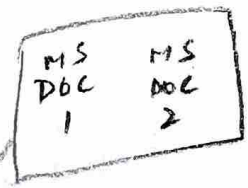


multiprogramming

Similar to multitasking but takes place in mainframe system & require specific programming

multitasking is coordinated by OS while multiprogramming requires specific written software.

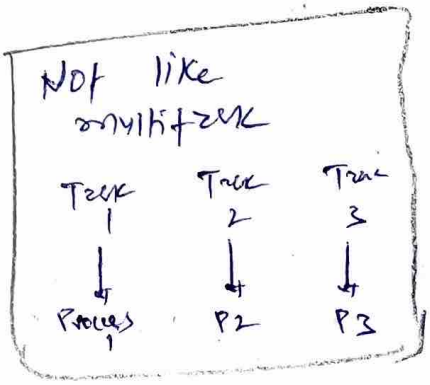
when an open 10 word doc is thread, each doc is process, 10 threads but one process

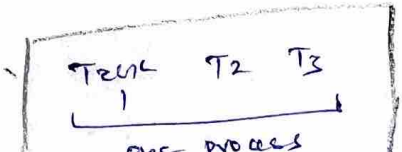


one APP, two threads

multithreading

Allows multiple concurrent tasks to be performed within a single process.





- context switching b/w active process reduce overhead, increase efficiency.

SMP send one thread to one process for simultaneous execution

Uses multithreading at OS level

2 types

SMP

- Symmetric multiprocessing
- simple operation at extremely high rates
- Processor share common OS + data bus + memory

MPP

- Massively parallel processing
- For large, complex, computationally intensive tasks
- Thousands of processors where tasks are further break into mini tasks, distributed to other processors & reassemble back again.

Processing Types

Design in such way = Doesn't disclose information to unauthorised clients

Other option is viz policy, and we have focus on hardware = processor level

Address this at PROCESSOR LEVEL

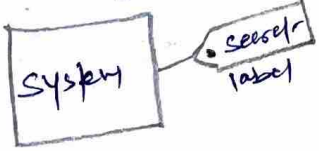
2 different ways

Through policy mechanism info. to manage info. at different levels

Through Hardware solution (Higher security)

SINGLE STATE SYSTEM

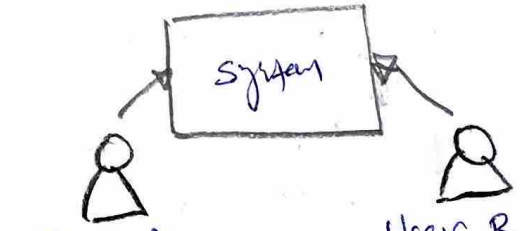
System admin approves processor + system to handle one security level at a time.



All users approved to handle secret information. This takes burden off to handle info. from → Administrators, Hardware, OS

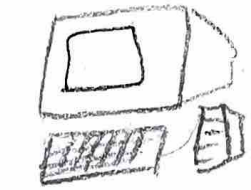
MULTI STATE SYSTEM

These systems are certified to handle multiple security levels simultaneously.



Technical mechanism prevents information crossing b/w two users (between two security levels)

Protection Mechanisms



switched-off = nothing. A piece of plastic

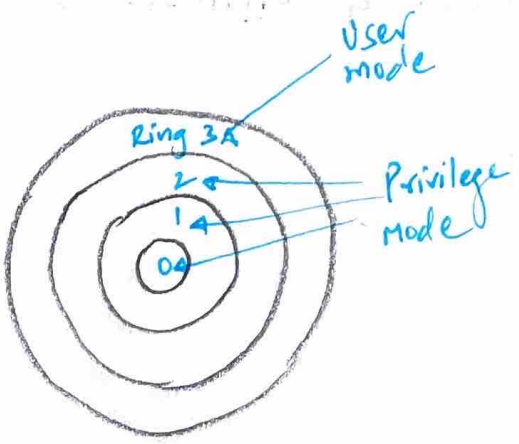
Computer

ON

Running computer has to address information security

Various protection mechanisms

1. Protection Rings
   - organize code & components in OS into concentric rings.



0-2 : Protection ring segregates OS into kernels, components & drivers

3 : This ring runs applications & programs. ↳ P.t.o

2. Operating states
   P.t.o

3. Operational ~~States~~ modes
   (1) User mode
   - CPU Access to small set of instructions
   - often executed in controlled environment such as VM.
   - Prevents user's unintentional action + malicious users intentions

   (2) Privilege mode
   - OS access to full range of instruction supported by CPU
   - wide range of permissions, Be careful when you give privilege access.

4. Security modes
   P.t.o x2

--- Protection rings (contd...)

Ring 0 is KERNEL

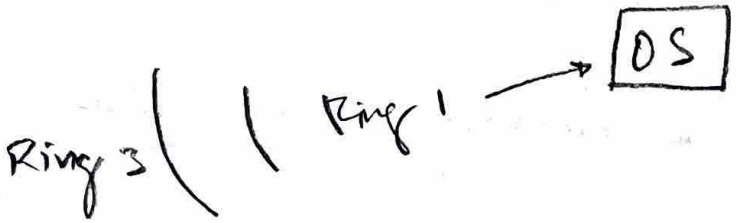
Lower numbered Ring = VIP
Ring 0 can access any resource / memory location.
To move access & interaction with OS

Higher numbered Ring = ordinary → less access

Ring 1 - OS components
Ring 2 - Drivers, Protocols

Mediated-access model (system call)

Ring 3 - User-level programs & Applications

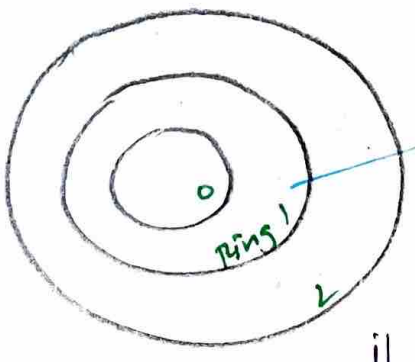


Ring 3 uses Ring 1 for handler / driver to access services in OS. Higher numbered rings need helper

Concept #

Ring model → OS to protect & insulate itself from users & applications

Concept #



Ring 1 can access resource in Ring 1 & 2
But not Ring 0.

if Ring 1 wants to Access Ring 0 -
it has to go via helper / system call / mediate- Access

2 Process states --- side concepts & part of protection rings

Operating states

→ Various forms of execution in which process may run.

OS in two mode of any given moment

Ring 0-2: Runs in supervisory or Privilege mode

Kind of Ring 3: user mode

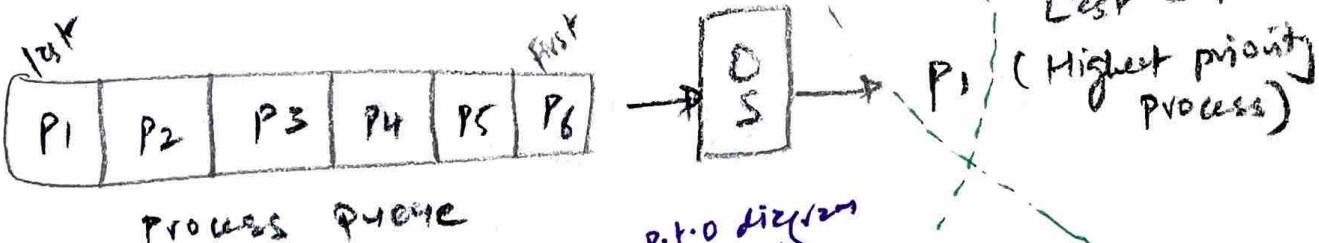
Supervisor state

Full-access

Problem state

low privilege

~~limited access~~



Process queue

P.T.O diagram

STATES

Ready (queue)

Process is ready to run. it has memory + resource

Running

a.k.a

Process continue to run until time slice expires or process is blocked. In these cases, process goes to ready state (queue) if time-slice expires

Process goes to waiting state (queue) if block while waiting for resource become available.

Waiting

Process waiting resource or device or access request

Supervisory

when process wants to perform privilege actions

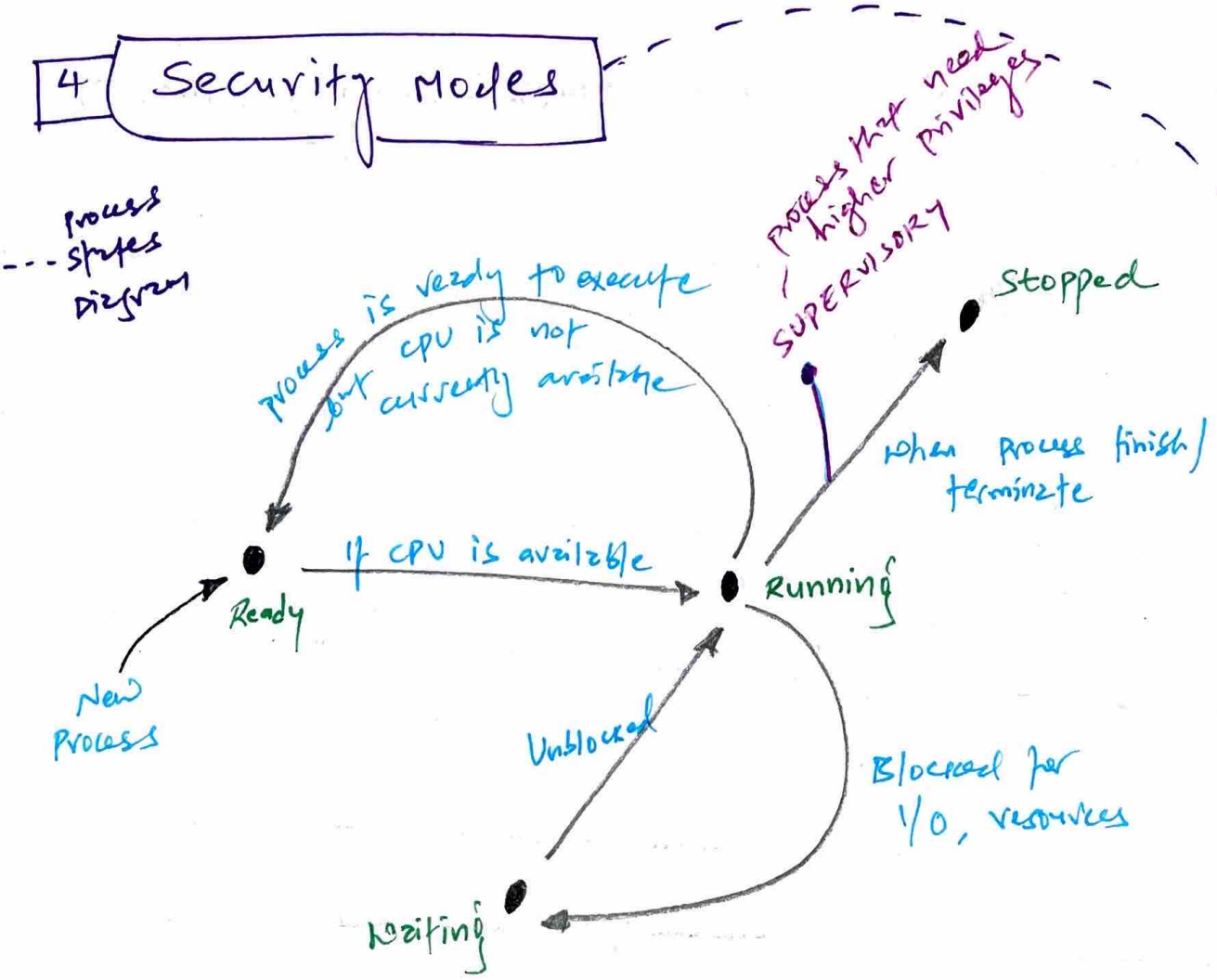
Stopped

Process is stopped when job is done or terminated.

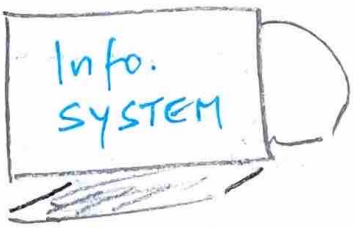
All resources + memory referred to it OS can use for other processes.

4 Security Modes

Process states Diagram



[Process scheduler Diagram]



To Protect

Four Security modes

(strong)
① Dedicated Mode
- similar to single state system
- valid Need to know
- Security clearance
- Access approval

(less strong)
System High Mode
"
"
3 requirements

diff :
- Need to know not necessary for all information processed by system.

(weak)
Compartmented Mode
"
No need for access approval for all information in system (need for any)

P.T.O CMW

(Weakest)
Multilevel Mode
Not everyone has security clearance.

CMW: Compartmented mode workstations

special mode implementation

2 forms of security label

Sensitivity levels

Which object must be protected

Information labels

Prevents data overclassification

Table - comparing Security model

Mode	Security clearance	Need to Know	PDMCL (if CMW is used)
Dedicated	Same	None	None
System High	Same	Yes	None
Compartmented	Same	Yes	Yes
Multilevel	Different	Yes	Yes

MEMORY

So far we learned PROCESSOR ← Hardware

Next (memory)

coming soon (storage)

ROM (Read-only memory)

can't be modified | No writing allowed

- Programmable ROM (PROM)
  - can be modified to some extent
- Erasable Programmable ROM (EPROM)
  - Ultraviolet EPROM (UEPROM)
    - Erase with light
    - End user can burn new information
  - Electronic Erasable EPROM (EEPROM)
    - EEPROM must be fully erased to be rewritten while HDD (memory) can be erased & written in blocks.
    - FLASH MEMORY
      - nonvolatile storage for electronic erase & writing
      - Use of electric voltage to erase data

RAM (Random Access Memory)

Power-off = volatile content = Temporary usage

- Real memory
  - Primary / main memory
  - largest storage on PC
- Cache memory
  - takes data from slower device & store to faster devices as cache to boost performance.

Sophisticated / Expensive — **Static RAM** — Faster

vs

Dynamic RAM — cheap / old

- Uses flip-flop as ~~Uses Set~~ logical device
- maintains contents unaltered as long as power is supplied

- Uses series of capacitors to store data

static / Dynamic = Volatile

---

lowest

Registers

- CPU's limited amount of onboarded memory
- Provide direct access to brain of CPU = ALU (Arithmatic logical unit)
- Advantage: this type of memory (Register) is part of ALU itself

Memory Addressing

- For processors to refer various locations of the memory

↳ **Register Addressing**: Small memory directly into the CPU

↳ **Immediate Addressing**: Not memory addressing scheme but how data is referred to CPU as part of instructions

↳ **Direct Addressing**: CPU is provided with actual address of memory location to access.

↳ **Indirect Addressing**: Memory address contains another memory address

↳ **Base + offset Addressing**

P.T.O

Secondary Memory

CD/DVD USB External drive

- Storage device that contains data not immediately available to CPU
- Inexpensive compare to primary memory, holds massive amount of information

Special kind

→ Virtual memory : Such as page file, OS uses for memory mgmt

→ Inexpensive but ~~sto~~ creates system slow

Paging operation occurs when data is exchanged b/w primary & sec. memory are ~~slow~~ slow.

Memory Security issues

FIRST UNDERSTAND

→ Where data is stored? (what kind of memory)

→ How it is stored?

If memory device store = Sensitive Data

↳ PURGE

(before they leave Organization)

Cyber Sketch

COLD BOOT ATTACK

— freeze memory chips

Attacks on memory image dumps or system crash dump to extract encryption keys.

Concern: Who will access data stored in memory while a computer in use

Data-in-use

Use this principle

PROCESS ISOLATION

Process don't have read / write access to memory spaces that are not allocated to them..

OSC P382

Implement VM per user / per process basis

III STORAGE

Terms

Primary vs. Secondary

- Don't confuse with primary & secondary memory but it's still same

PRI MEM	→	PRI STO = RAM
SEC MEM	→	SEC STO = CD/DVD

(Faster) — Random vs. Sequential (slower)

Hold massive storage = good for backup

~~Power-off → Data loss = Volatile~~

Random = Primary storage device + secondary

Allows OS to read/write anywhere / any point

Sequential = Magnetic tape = read/write data in sequential order

Volatile vs. Non-Volatile

Power-off ⇒ Data lost = Volatile (static / dynamic RAM)

NO Data loss = Non volatile (magnetic tape)

Storage media Security

3 concerns for secondary storage devices

Theft (Economic loss)

Ensure full disk encryption

Data Remanence

- Traces of data remains after erasing / formatting
- Perform Sanitizing

SSD ⟷ sanitization ?

Traditional ZERO-WIPE is ineffective as data security measure for SSDs

Availability

Ensure data is retained (Back-up) with protection when we need it

Access to data stored in secondary storage device

- OS level controls
- IAM
- Encryption technologies

Input / output devices

- Monitor
- Printer
- Keyboard / mice
- Modem — who use this?

FIRMWARE

microcode

A software stored in ROM chip.

2 Types

BIOS on motherboard

Basic Input/output system = instruction to load OS from disk & start PC

- Stored in EEPROM
- Flashing the BIOS = process of updating BIOS

Internal and External device firmware

- Mini OS as firmware in device such as Printers, Canon c100
- stored in EEPROM = easy to upgrade

Remember
BIOS = EEPROM

Phishing

Malicious code embedded into BIOS firmware = can remotely control the device

* 2011 UEFI replaced BIOS

Unified Extensible Firmware Interface, advanced interface b/w hardware & OS

CLIENT-BASED SYSTEMS

client-side Attack on

Example

Malicious website


User


Data


System

2 things

APPLETS

mortgage calculator

- Code objects sent from server to client to perform some action
- They are not gone, browsers still support = security risk

How?

Using Java Applets

Remote system send code to local system for execution, if (code) could be trojan.

↳ mortgage calculator

- Financial data from user could capture & send to server without consent.

LOCAL CACHE

- Any data temporarily stored on client system for future use / reuse.

local cache

- ARP cache
- DNS cache
- Internet File cache

P.1.0 x2

Poisoning

Applet types → P.1.0

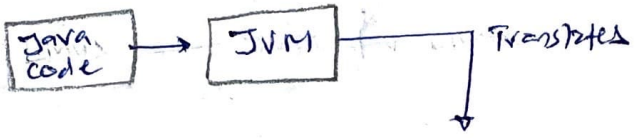
Applet types

JAVA Applet

Problem → Need multiple compilers to produce different version of single application for each platform it must support.

Soln = Java virtual machine (JVM)

Each system that runs Java code downloads the version of JVM supported by its OS.



JVM

Benefit : code can be shared b/w different OS without modification

Container is one step ahead — deal with only one OS!

Sandbox concept ← To Address security

Java code isolate from OS & strict controls perform on what resources ~~that~~ those objects can access.

Active X controls

Bad = outdated

- Microsoft's answer to Sun's Java applet

① Active X = Proprietary only runs on Microsoft Browser

② Active X ∉ Sandbox
→ They have full access

Be careful before downloading Active X & exactly the.

contd.. Local Cache

DNS Cache Poisoning

ARP Cache Poisioning

MITM Attacks

Mitm: man-in-the middle attack

Kali's Ettercap.

Poisons dynamic ARP Entries (10 min)

- Static ARP Poisions = Permanent, even after reboots

(1) Static Host file

- Attacker tamper / inject false info b/w FQDN & IP Address relation for permanent damage

(2) Authorised DNS server Attacks

Not effective

- Primary record of FQDN is stored on primary authoritative DNS server = Propogated to Internet

Try this

(3) Caching DNS server

- Most ISP cache contents.

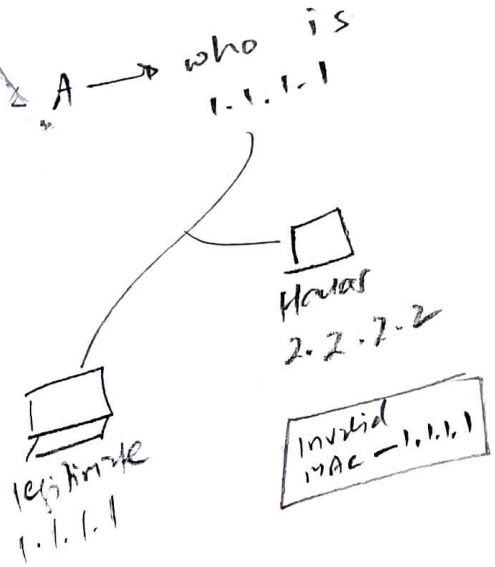
Kaminsky DNS vulnerability

(4) Alternate DNS IP

- clients get wrong DNS IP Address

(5) DNS Query spoofing

- Similar to MITM Attack



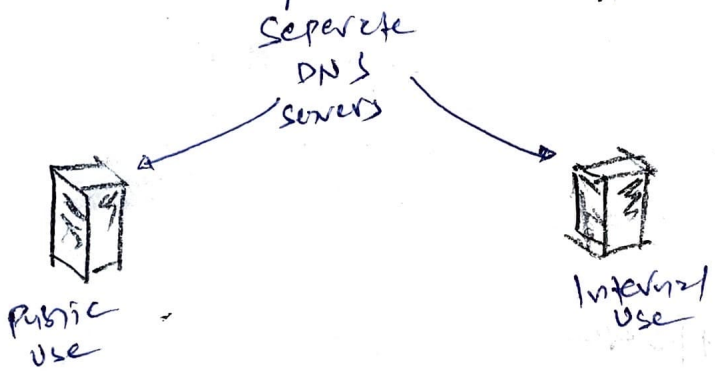
Temporary Internet Files (Internet file cache)

- Website content / downloads
- Split Response Attack : client downloads files from unintended web page.
- Mobile code scripting Attack: plant false content in cache

Keep OS + Apps with latest patch — solves

Use SPLIT-DNS system (split-brain)

a.k.a Split Horizon



SERVER BASED SYSTEMS

Focus / concern is

DATA FLOW CONTROL

Movement of data b/w process, devices, across the network / channels.

considers

- Transmission of Data
  - latency
  - throughput
- Info. protection
  - CIA
- system is not loaded with too much traffic
  - load Balancer

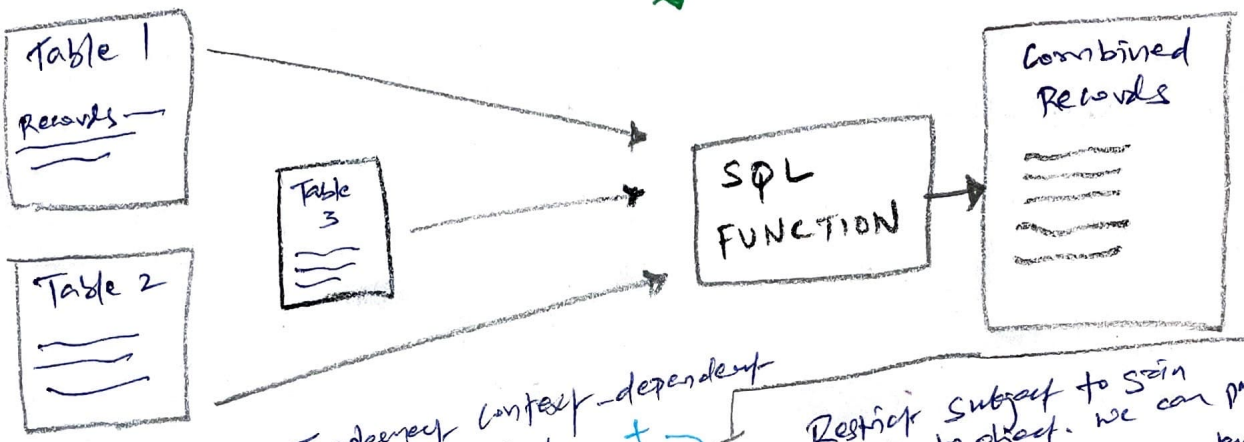
- DDoS Attack
  - Severe detriment of data flow control
    - protection mechanism (ch: 12 to 17)

DATABASE SYSTEM SECURITY.

Aggregation | Inference | Data Mining + Data Warehousing | Data Analytics

1 AGGREGATION

→ Combines records from one or more table to produce useful information.



Implement context-dependent Access control + → Prevention: Restrict subject to gain access to object. We can put object into higher clearance level so lower clearance subject can't access

Aggregation Attacks

Low-level security items / value + → Polymorphism → creates higher security level / value

EXAMPLE

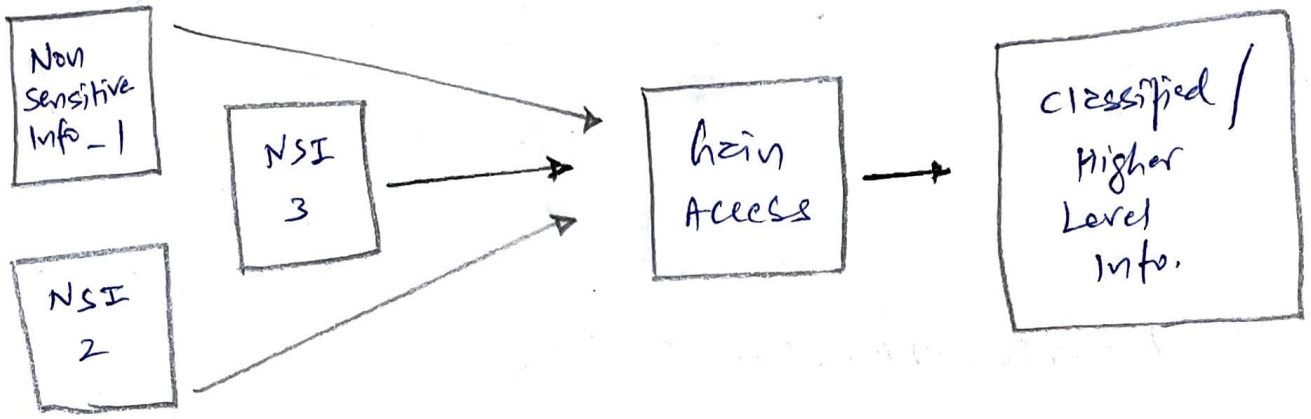
Low-level Military clerk → Access to → Equipment Inventory + transfer generals from base to base

Aggregated Function = clerk knows how many troops are assigned to each base station.

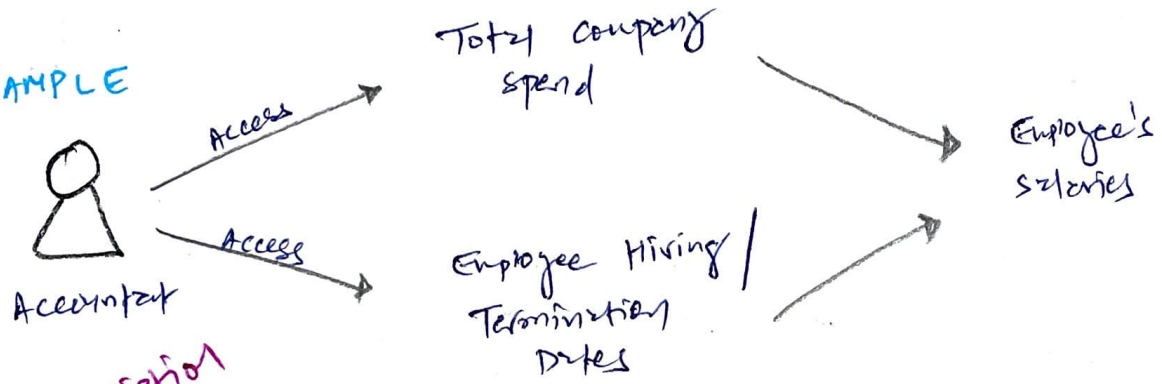
SENSITIVE INFO FOR ENEMY → Requires restricted database access.

2 INFERENCE

is intended result of Aggregation



EXAMPLE



Polyinstantiation

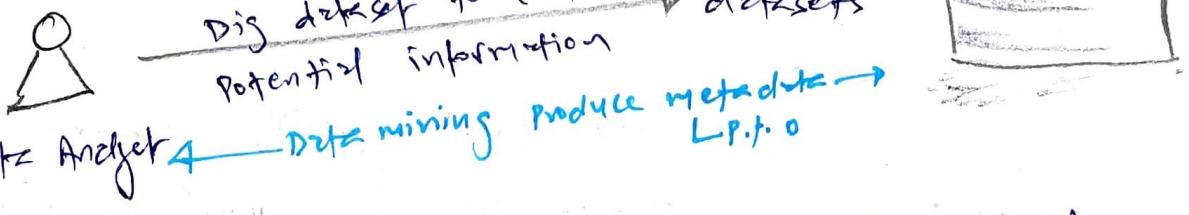
Defense / Protection

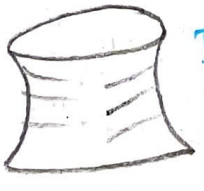
- cell suppression
- Database partitioning, noise & perturbation
- Intentional blurring of data
- least privilege

P.t.o End bigger picture

Vulnerable to attack 1 & 2

3 DATA MINING & DATA WAREHOUSING





Data Dictionary - critical information about data, usage, type, relationship, format & sources.

Metadata

- Data about data. Info. about data.
- Can be subset / superset of large dataset.

Example – Security Incident Report
Metadata extracted from large dataset of audit logs

- - Metadata is sensitive = Security concern

↓

Stored in secure container called

DATA MART

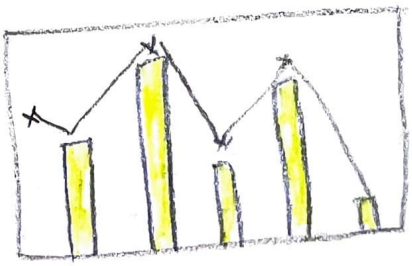
4 DATA ANALYTICS - - - - **BIG DATA**

Challenges

mgmt →
- Collection,
- Storage,
- Analysis,
- Mining,
- Transfer,
- Distribution

security →
- Data breach,
- Addressing compliance
- Detecting violations
- Improving efficiencies
- Improving productivity

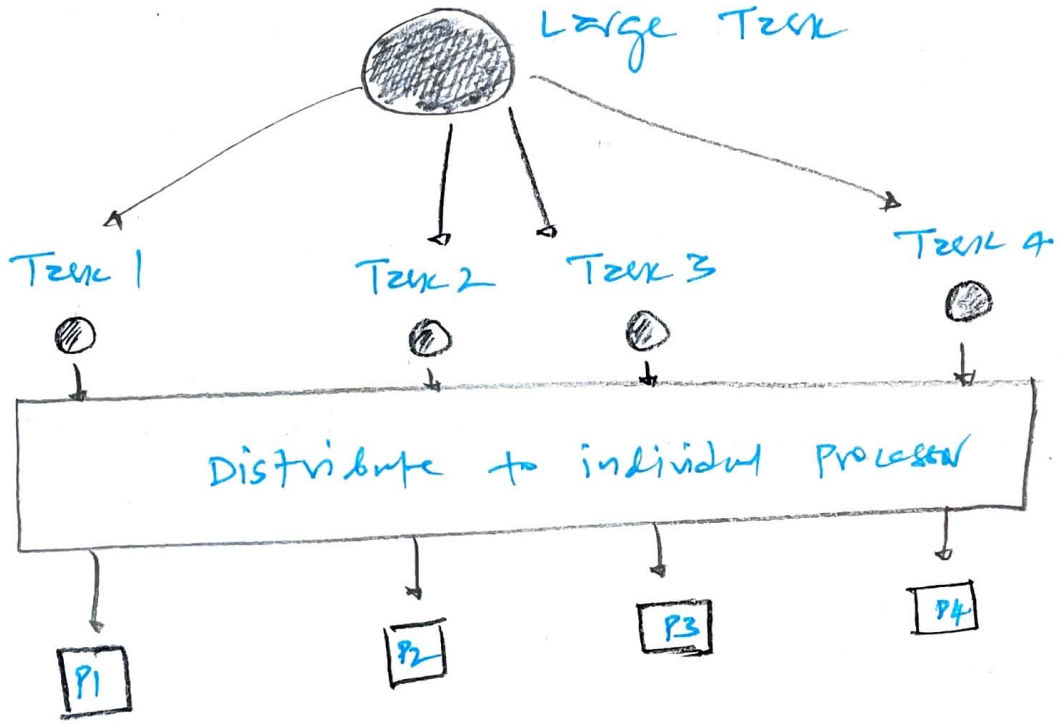
Extract useful information from bulky datasets that make sense / insights for Business



LARGE-SCALE PARALLEL DATA SYSTEMS

Parallel Computing — multiprocessing

Computational system designed to perform numerous calculations simultaneously.



Multiprocessing Divisions

Symmetric multiprocessing (SMP)

- Processor share same OS & memory
- collection of processors works on same task, code or project.

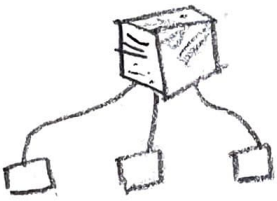
Asymmetric multiprocessing (AMP)

- Processors & OS are independent of each other
- Each processor has its own OS & task

- Under AMP, processors are configured to execute specific task / code, it's called Affinity in some circumstances.

DISTRIBUTED SYSTEM AND ENDPOINT SECURITY

Evolution of Computing



Host / Terminal Model

Client-Server Model

Distributed Architecture

- Prone to vulnerabilities in monolithic host / terminal system
- Communication equipment can be unwanted points of entry to distributed environment.
  - router / switch / modem
- User = threat if downloaded malicious code / trojan horse
- Data on machine = risk if not properly backed-up.

Security concern

Process + storage distributed on multiple clients & servers = Everything must be secured.

Virus spreads faster in distributed compare to monolithic architecture

To safeguard Distributed Environment means

Understand Vulnerabilities + Risk

Security controls

- Technical
- Policy, process + procedures