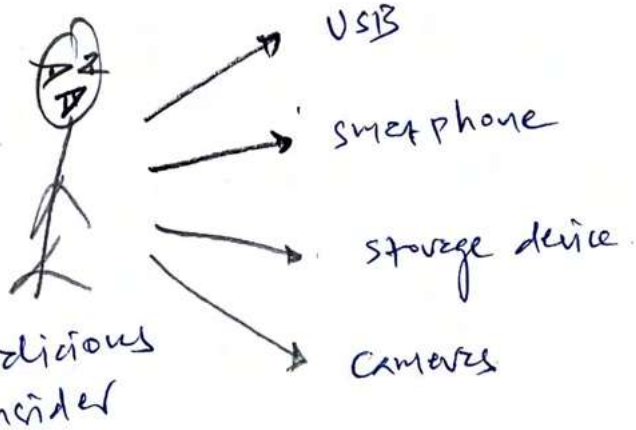
ASSESS AND MITIGATE VULNERABILITIES IN MOBILE SYSTEMS



To steal internal confidential data & expose to outside world

⇩

WIKILEAKS

Dangers of Mobile Devices

- Camera to capture sensitive information
- USB connection to transfer files/ photos/ video
- Eavesdropping conversations
  - Be careful when talking in public place

Mobile Security

Device Security

No value of feature till they are enabled

Full Device Encryption

- Good feature but useless if device is stolen or system has backdoor vulnerability
- Voice encryption makes eavesdropping useless.

Remote wiping (Remote sanitization)

- If device is stolen but no guarantee of data security
- Encrypt device so even after recovery, attack struggle to decipher

Erase all data if incorrect code entered 10 times

Lockout

3 attempts = Account | device is locked

Screen Locks

Pattern, PIN, FaceID

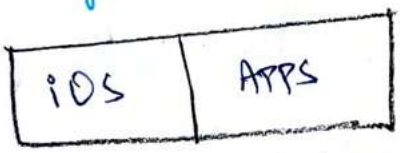
GPS

- Find my iphone

Application control

- Limit which APP can be installed = reduce exposure for malicious apps

Storage segmentation



Mobile device

- Artificially compartmentalize various types of data on a storage medium

Asset Tracking (Active / passive)

To verify that device is still assigned to authorised user. Prevent | locate missing devices.

Inventory Control

Mobile camera = scan bar codes to track physical goods

Mobile Device Management (MDM)

manage
- BYOD
- company device

security, mgmt, monitoring & troubleshooting of devices

Device Access control

- To reduce unauthorised access
- MDM to force screen-lock configuration

Removable storage

Mobile → micro SD
Mobile → USB
Mobile → Bluetooth / Wifi

Disabling unused features

- Turn-off SIRI
- Disable location based service

Application Security

Key management
- Don't store keys locally on mobile. Consider TPM or removable hardware
- Google KMS
  - ↳ Hashicorp Vault

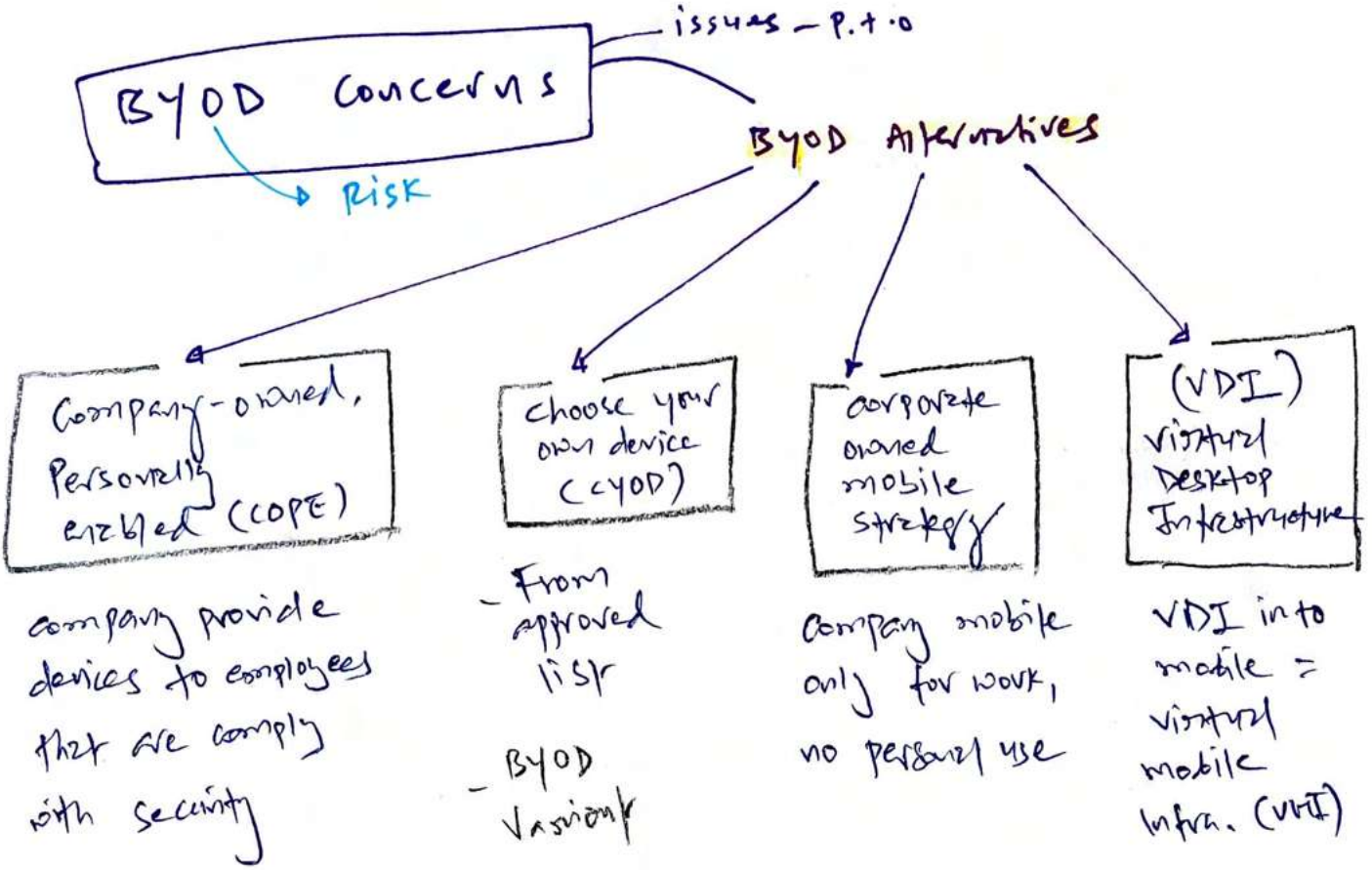
Geotagging
Don't like Insta Photos & Google reviews attached with locations

Credential management
- Cyber Ark

Encryption
- At Rest
- In Transit

Authentication
To combine
- Consider multi-factor authentication + device encryption

Application whitelisting
- Implicit deny
- Prohibit unauthorised software from being able to execute.



BYOD Related Issues

Data Ownership

Problem
- Have a clear policy as remote wipe of business & personal data = individual's significant loss

Solutions
- MDM solution = data isolation + segmentation
- Backup solution of personal & business data in case of remote wipe

reduce the risk of data loss in event of remote wipe / device failure / damage

Support Ownership

- Policy for = if employee phone → theft / repair / damage

who will do it?

Patch Management

- Policy for mobile device updates
  - is user responsible?
  - Enforce patch / updates

Antivirus management

- Policy should dictate which Antivirus installed on mobile device

Forensics

- Make mobile user aware = device will involved in case of security violation / crime

Privacy

- Policy should address privacy & monitoring
- Employee to agree of tracking work mobile after business hours.

On-boarding / off-boarding — have policy for both

- On-boarding
  - Install / keep update
  - Security input
  - Business Apps
- off-boarding
  - Full wipe
  - Factory Reset

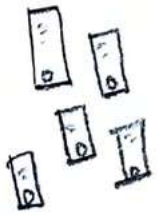
Adherence to corporate Policies

Personal ~~work~~ mobile as BYOD work
- comply → work + security policy
- → x Tinder / personal use

User Acceptance

organization → Educate About Personal mobile Policy → User → Acceptance → on-boarded

Architecture / Infrastructure Considerations



Move personal BYOD mobile Device
- → Increase Infra cost $$↑
- → IP Assignment
- → Load on IPS / IDS
- → Bandwidth consumption
- → Wifi congestion / interference

Legal concerns — Attorney has job to do!

Personal Devices for Business Activities
- → Increased burden of liability
- → Risk of data leakage

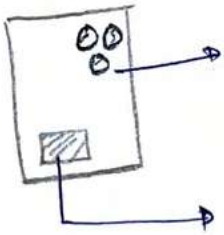
AUP : Acceptable Use Policy

Users to Accept

Company policy (or) Personal Device policy

Restrict user to access inappropriate content + information disclosure

On-board camera / video + storage



when not to use camera

what they can / can't store

define in policy

Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems

Don't offer new / surprising elements

Static Environment / system

Conditions / Events that don't change = Reduce risk / security

Embedded System

- Designed around a limited set of specific functions in relation to larger product of which it's a component.

N/w enabled devices:
- Smart appliances, smart TV
- medical devices,
- n/w attached printers

OS
h/w
s/w
n/w
→ configured for specific need / function & set to remain unaltered

Examples of embedded & static systems

Cyber-physical systems
- Robotic = movement element
- Sensor = physical condition

Extension = IOT

Devices that offer means to control in physical world.

Main frame systems
- Perform high complex calculations & provide bulk data processing

Home consoles

Vehicle-computing systems → TESLA

No hear about security? — P.T.O

IOT
P.T.O End

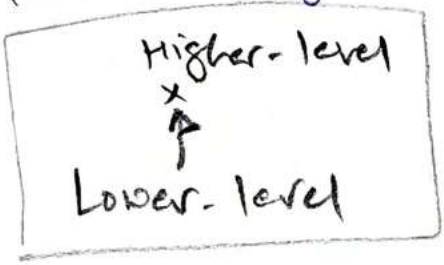
Methods of Securing Embedded and Static Systems

Network Segmentation

- Assign different network range for IoTs.
- VLAN, Application filtering, Routing, Access control mgmt.

Security Layers

- different level of classification / sensitivity grouped together & isolate from other group.



- Isolation
  - Physical = N/W segmentation, Air Gaps
  - Logical = classification

Application Firewalls + Network Firewalls

Manual updates

- First read release notes before upgrade / downgrade

Firmware Version Control

Wrappers = controlled channel to check integrity & authenticity before manual updates are applied

Monitoring - SIEM

Control Redundancy & Diversity = Availability

Build-in security solution = Defense-in-depth

ESSENTIAL SECURITY PROTECTION MECHANISMS

Everything starts from here:

Software should not be trusted.

⇓

SECURE ARCHITECTURE

Technical Mechanisms

- Layering
  - similar to Ring model
  - centre of ring = Highest level = more privileged
  - Lowest = least privileged
  - sensitive info = core circle
  - less secure info = outer rings
- Abstraction
  - ~~Access control per groups~~ (AD Groups)
  - P.I.O - Revised misunderstood End
- Data Hiding = containers
  - multilevel secure system
  - Placing objects in security containers (logical)
- Process Isolation
  - OS enforce process seperation with dedicated memory space
  - VM
- Hardware Segmentation (physical)
  - Same enforcement as process but use of physical hardware

Policy Mechanisms

- Principle of Least privilege
  - Run in user mode whenever possible
  - More process in privilege mode = VM + malicious ↑↑
- Seperation of Privilege
  - Least privilege for Administrators.
  - Builds on top of least privilege
  - Granular level access = Permission per privilege
- Accountability
  - Need authorization & authentication system + Auditing & monitoring system

Common Architecture Flaws and Security Issues

Covert channel

Road less travel : a path not usually for passing information because it's not protected by system's normal security controls.

covert timing channel

- Pass information by altering resource's timing
- secretly transfer data, hard to detect

covert storage channel

- convey information by writing data to storage so other process can read it.

Defense to covert channel = Audit & Analyze log files of covert channel

* Attacks Based on Design or Coding Flaws and security issues

- Seperate testing for security issues = Pending.

P.t.o → common attack source or vulnerability of security architecture

↳ Trusted Recovery

- Ensures security controls remain intact in the event of system crash.

→ Database crash while writing data classified as top-secret

↳ unprotected system = unauthorised access

→ Trusted Recovery = ensures no confidentiality violation occur during crash

↳ Input and Parameter checking

Most notorious security violation = buffer overflow

- Happens when we don't have sufficient limit on input data
- Programmers to blame who ignore proper data validation in the code

↳ Maintenance Hooks & Privilege Programs

Back Doors = only developer know the hidden entry point in the system

originally designed for maintenance activity

Common system vulnerability = Practise of executing a program whose security level is elevated during execution.

↳ Incremental Attacks

slow, gradual incremental attacks

DATA DIDDLING

- Subtle damage on system storage, input/output
- Hard to detect unless files are protected from integrity check or encryption
- Tripwire : good tool to address data diddling

SALAMI ATTACK

- Metaphore : stealing thin slice of salami by customer each time
  ↯
  deducting small amount from financial records routinely.
- Defense : seperation of duties + proper control over code

↳ Programming - other flaws

Programs that doesn't handle exception well = unstable state

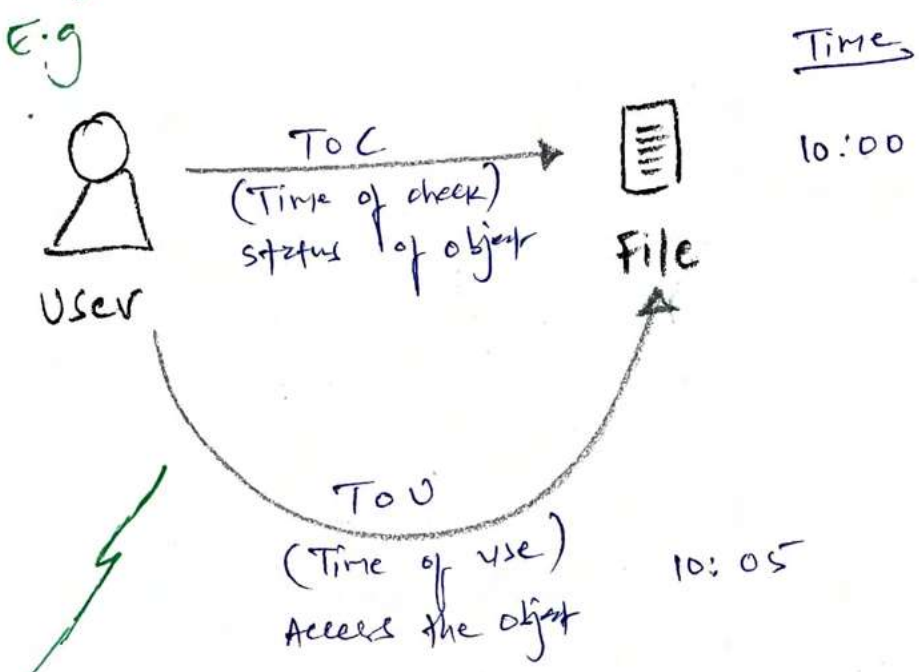
If attacker successfully crash the program = ↓ gain
Get high-security level = ↓ consequence
CIA compromise

Write a secure code. Difficult. Not impossible.

Install latest version of software & be aware about existing vulnerabilities

↳ Timing, State changes, and Communication Disconnects

Attackers attack based on predictability of task execution (repetitive task)



Attack based on Timing

TOCTTOU (Race conditions) — gn this A minute of time difference, attacker can replace normal file with malicious code.

Communication Disconnects — Small window of opportunity when attacker exploit

System state — Attacker attempt to trace action b/w two known states when state of resource or entire system changes.

State Attacks

↳ New Technology and Process Integration

Intertwine for new business function

=

Security problems

⇓

Focus

Single point of failure

Emerging weakness in Service oriented Architecture (SOA)

SOA is BAD ~~bad stuff~~

- SOA constructs new APP | functions out of existing ~~soft~~ but seperated software services.

New deployment / function = must be Securely evaluated & tested

Ls Electromagnetic Radiation.

Emanation leaks

→ Intercept to recreate keyboard input, monitor output

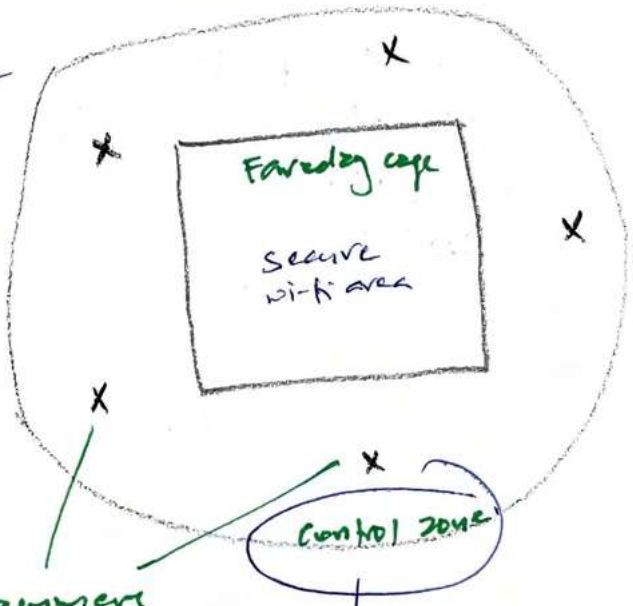
Sol.

Jamming

Noise Generators

Faraday cage

Control zone



Jammers

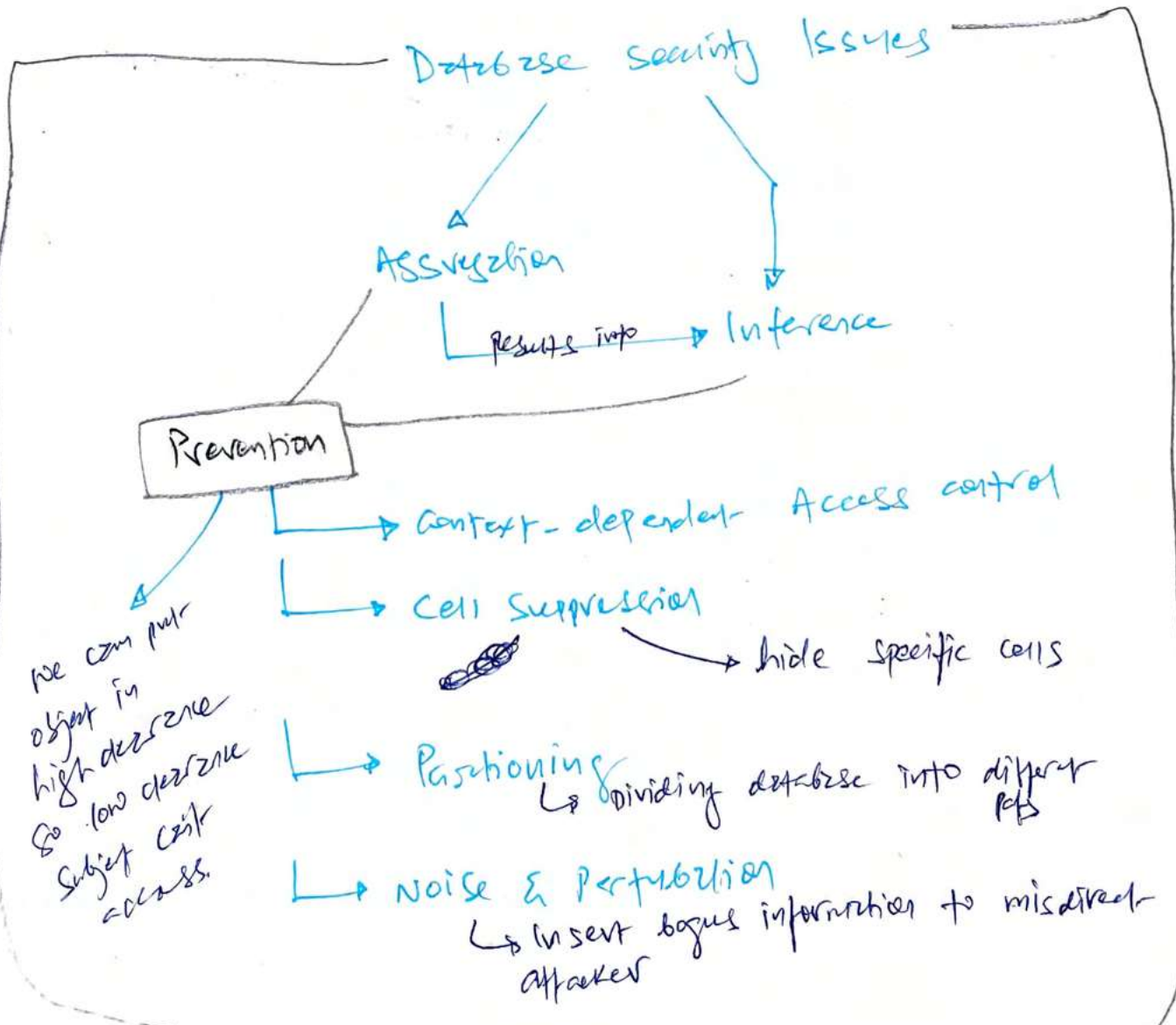
Wireless device works within control zone & blocks encryption outside

finally.

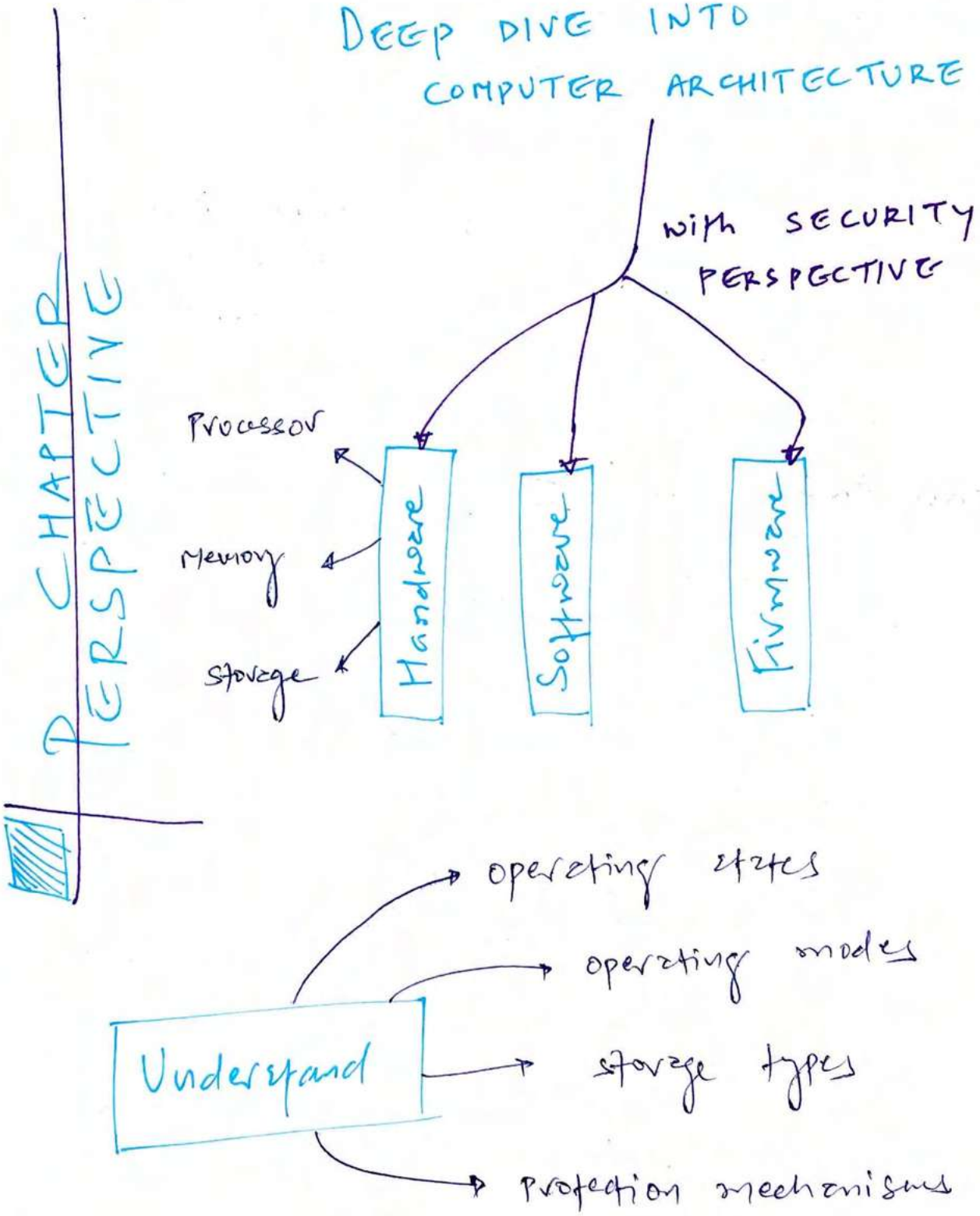
Abstraction = Black Box = Object

- Fundamental principle behind object-oriented programming
- It is Black Box Doctrine
- Core concept: Users of the object don't need to know how object works or how object is implemented.

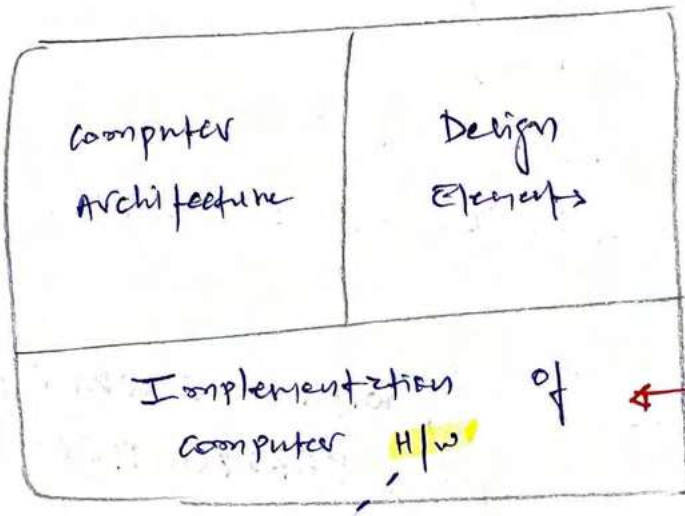
Black-Box Approach



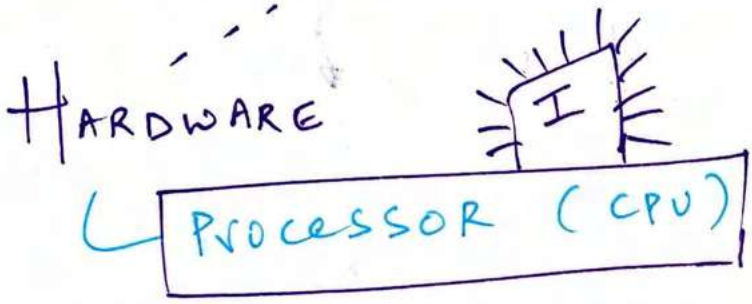
9. SECURITY VULNERABILITIES, THREATS, AND COUNTERMEASURES.

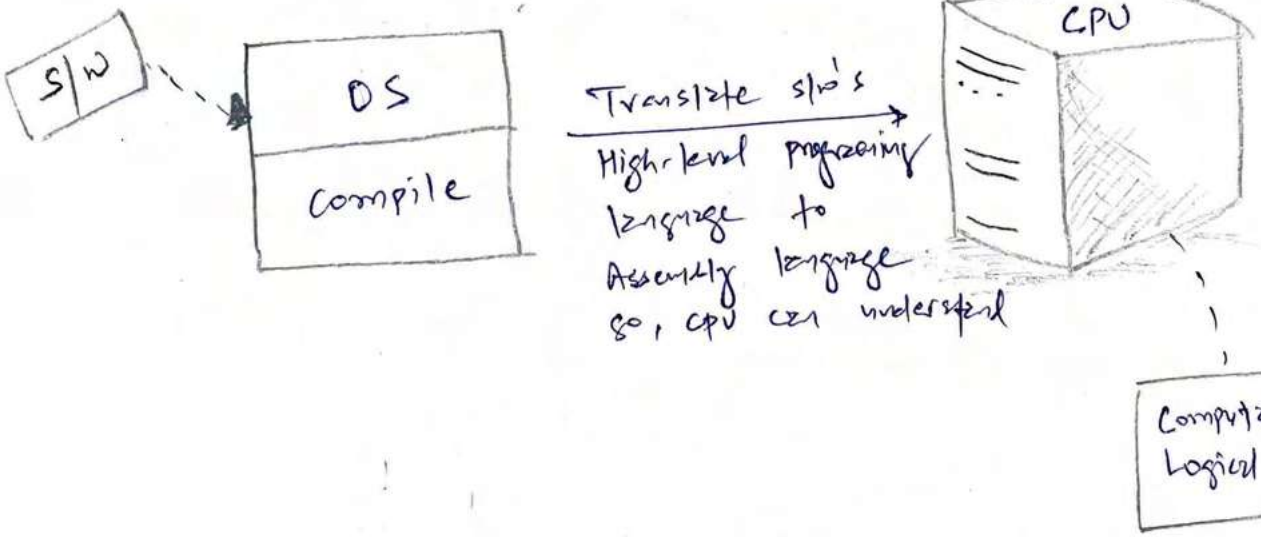


ASSESS & MITIGATE SECURITY VULNERABILITIES



Foundational Understanding of CISSP





Move Demand = Move Power = Advanced Features

→ Execution types (P.T.O)

Execution Types

Multitasking

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

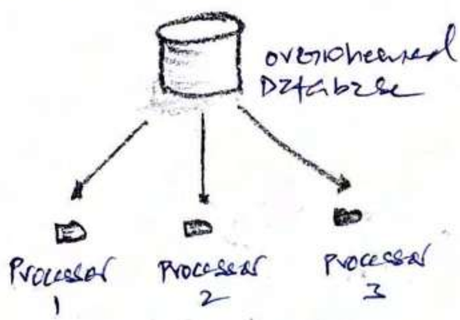
multiprogramming

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

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

multiprocessing

More than one processor to increase computing power.



2 types

SMP — Uses multithreading at OS level

SMP send one thread to one process for simultaneous execution

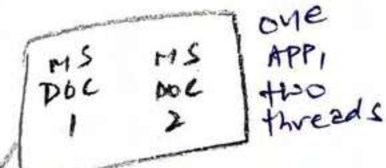
- Symmetric multiprocessing
- simple operation at extremely high rates
- Processor share common OS + data bus + memory

MPP

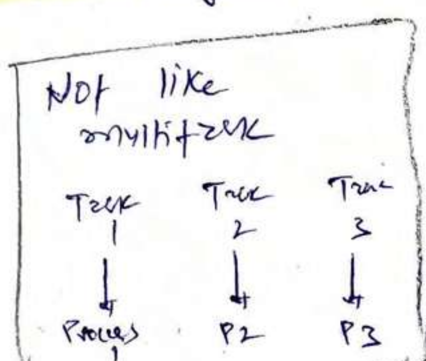
- Massively parallel processing
- For large, complex, computationally intensive tasks
- Thousands of processors where tasks are further break into mini tasks, distributed to other processors & reassemble back again.

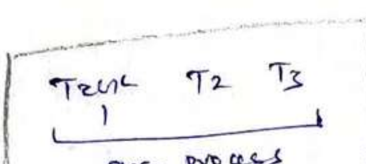
multithreading

when we open 10 word apps - Each doc is thread / 10 threads but one process



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





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

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. manage to manage at different levels

Through Hardware solution (Higher security)

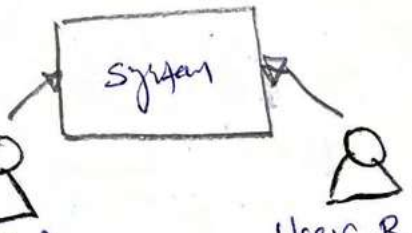
SINGLE STATE SYSTEM

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

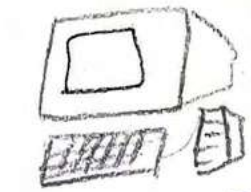
MULTI STATE SYSTEM

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



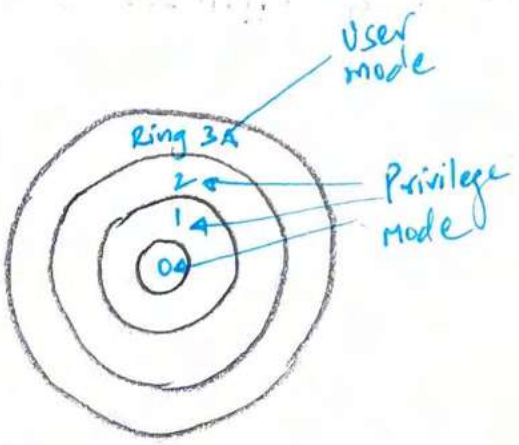
Computer ← switched-off = nothing. A piece of plastic

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...)

Lower numbered Ring = VIP

Ring 0 is KERNEL — 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)

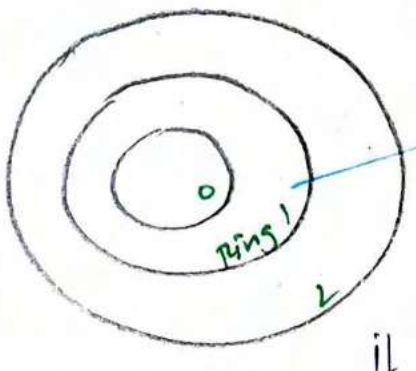
Ring 3 - User-level programs & Applications

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 — Operating states

--- side concepts of page of protection rings

↘ Various forms of execution in which process may run.

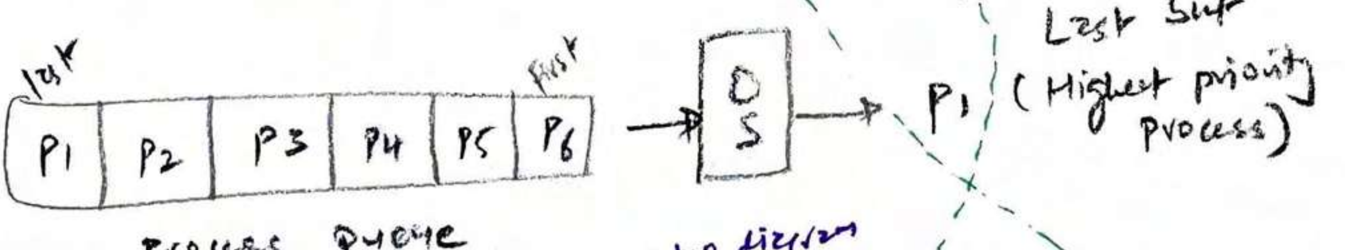
OS in two mode at any given moment

Supervisor state — Full-access

Ring 0-2: Runs in supervisory or privilege mode

Problem state — low privilege ~~limited access~~

kernel of Ring 3: user mode



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.

Supervisory
when process wants to perform privilege actions

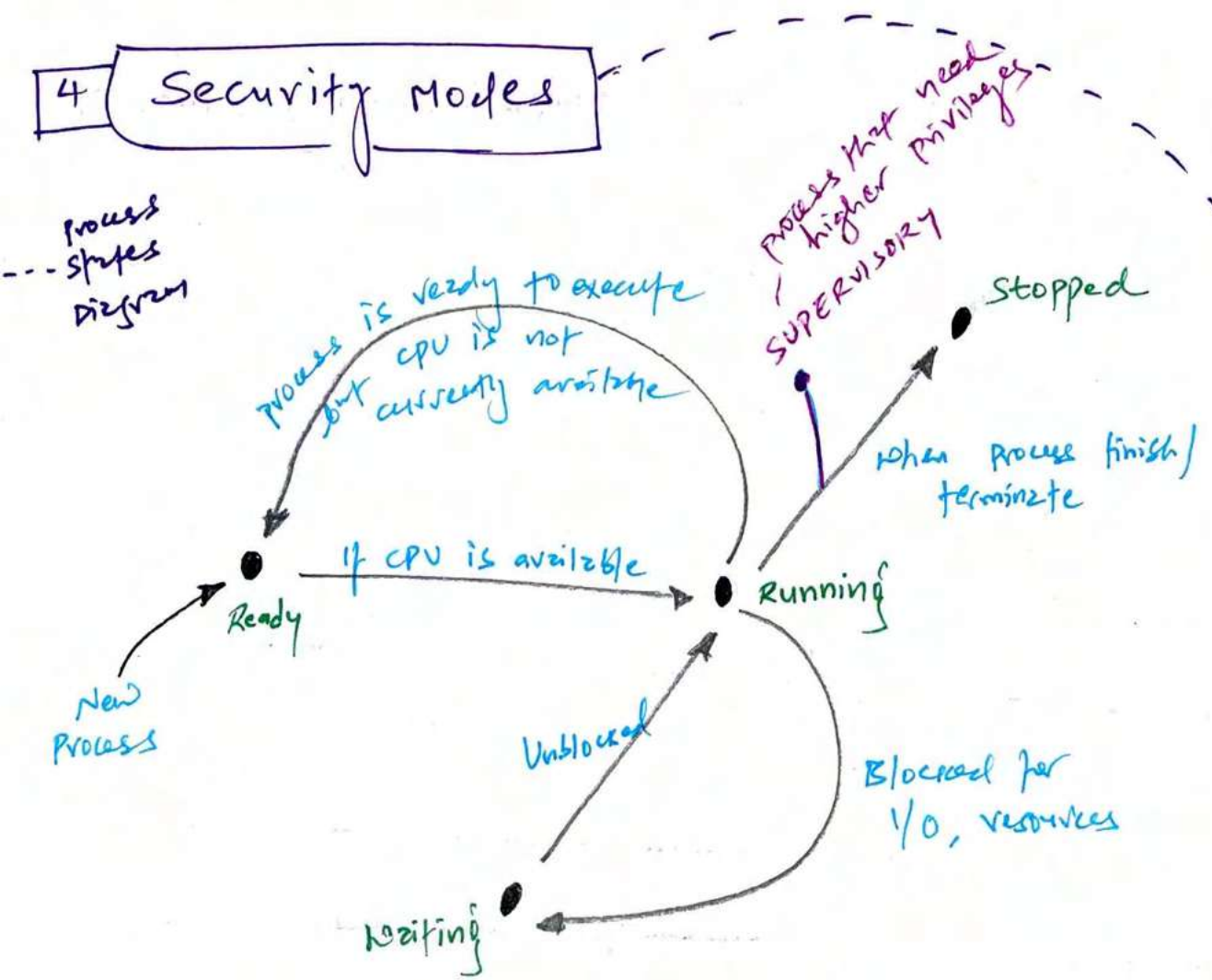
Waiting
Process waiting resource or device or access request

Stopped
Process is stopped when job is done or terminated.

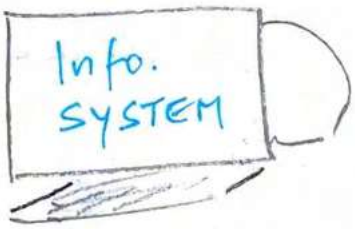
All resources + memory released so that OS can use for other processes.

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 approvals

(less strong)
System High Mode
" "
" "
3 requirements

(weak)
Compartmented Mode
"
diff: No Need for access approval for all information in system (need for any)
↓
P.P.O CMW

(Weakest)
Multilevel Mode
Not everyone has security clearance.

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

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 semi~~ 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 p 382

Implement VM per user / per process basis

STORAGE III

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 + secondary storage device, 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

Phlashing

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

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, it (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

Positioning

Applet types → P.1.0

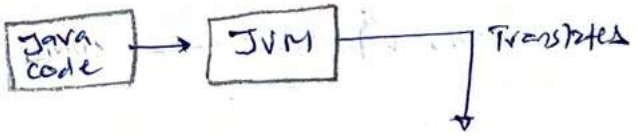
Applet types

JAVA Applet

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

① Static Host file
- Attacker tamper / injair false info b/w FQDN & IP Address relation for permanent damage

Mitm: man-in-the middle attack

Keli's Ettercap.

Poisons dynamic ARP Entries (10 min)

- Static ARP Poisions = Permanent, even after reboots

② Authorised DNS server Attacks

Not effective

Try this

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

③ Caching DNS server
- Most ISP cache contents.

Kaminsky DNS vulnerability

④ Alternate DNS IP
- clients get wrong DNS IP Address

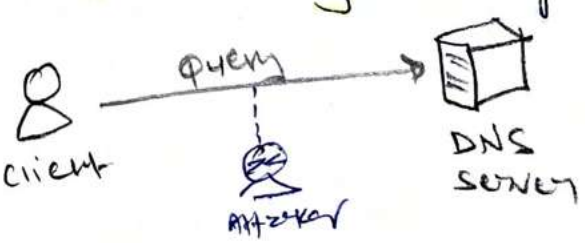
A → who is 1.1.1.1

Hacker 2.2.2.2

Invalid MAC — 1.1.1.1

legitimate 1.1.1.1

⑤ DNS Query Spoofing



- Similar to MITM Attack

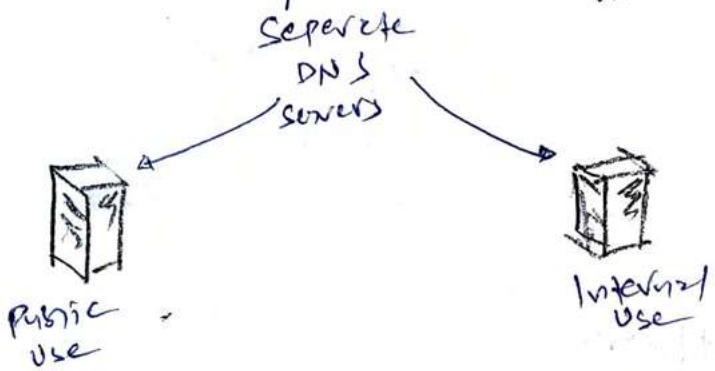
Temporary Internet Files (Internet file cache)

- 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

|

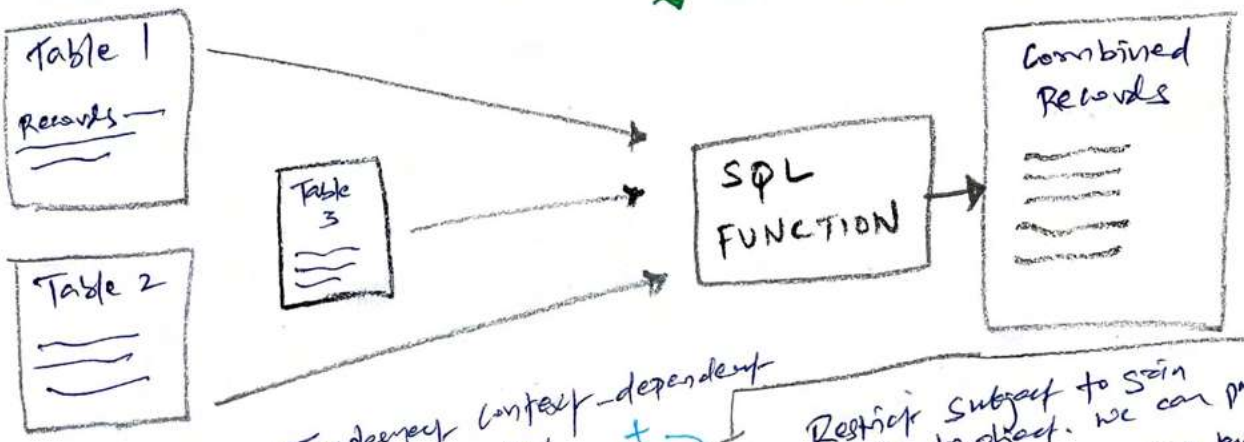
|--- protection mechanism (ch: 12 to 17)

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

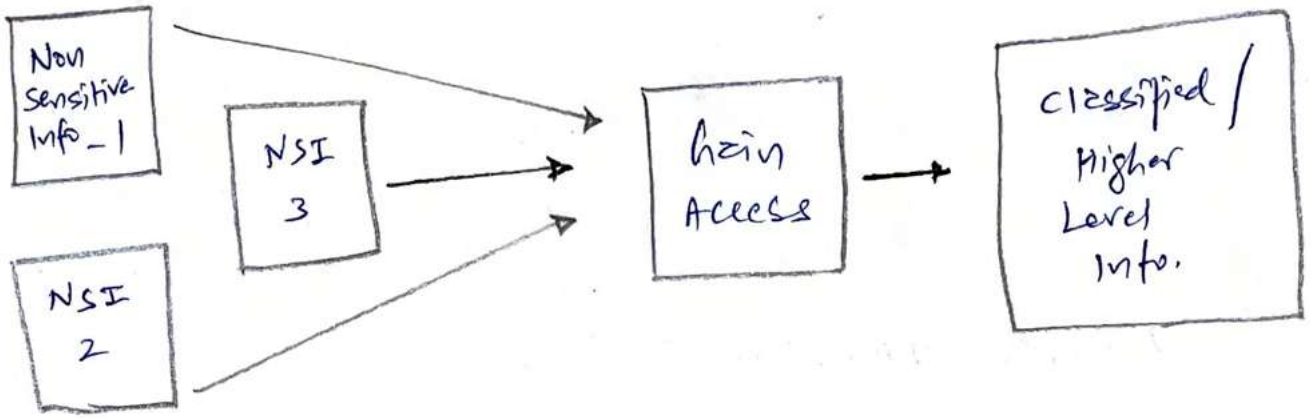
EXAMPLE

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

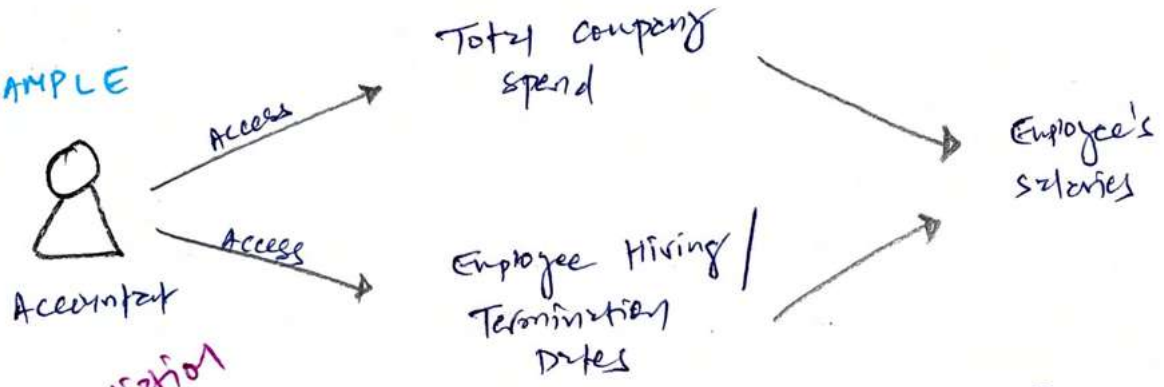
Aggregated Function = clerk knows how many troops are assigned to each base station.

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

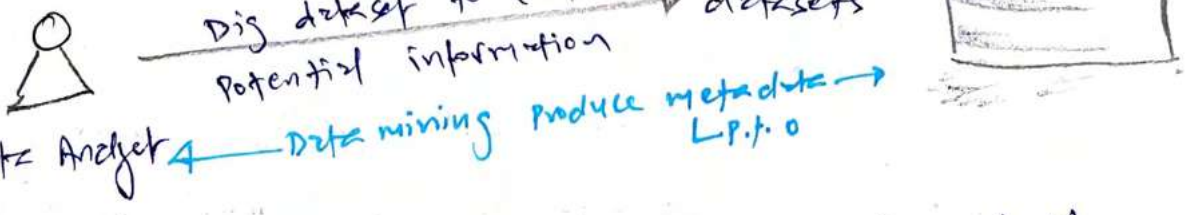
→ Intentional blurring of data

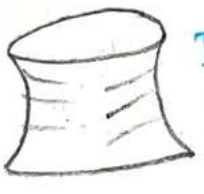
→ least privilege

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

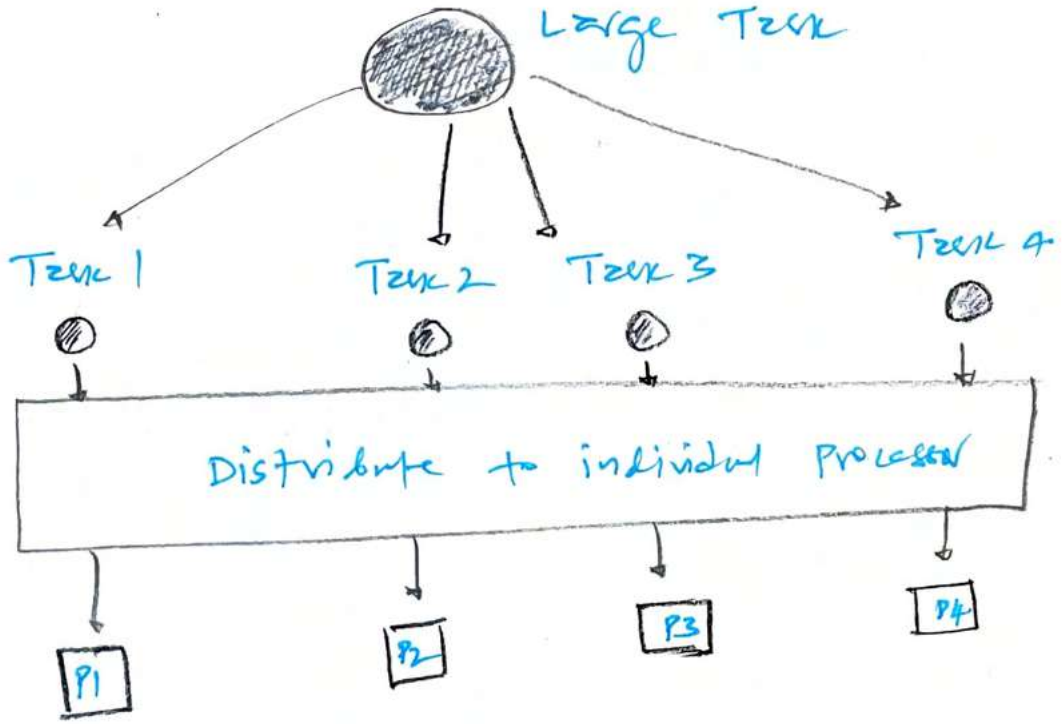
Data breach,
Addressing compliance
Detecting violations
Improving efficiencies
Improving productivity

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.

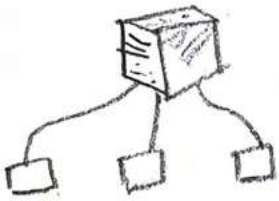
Asymmetric multiprocessing (AMP)

- 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

- Structure of Common Criteria

- client initially selects vendor based on published EAL - Evaluation Assurance Level.

3 AREAS :

- Part 1 — General concepts for evaluating IT security
- Part 2 — Security functional requirements
- Part 3 — Security assurance requirement for TOE

P.T.O

End — EAL = information that appears on various CC documents are the evaluation assurance levels.

EAL Levels (IMP)

STANDARDS

- CC → System security standard
- PCIDSS → Secure transaction + Financial data
- ISO → Standard for commercial equipment, S/W, protocol, manager

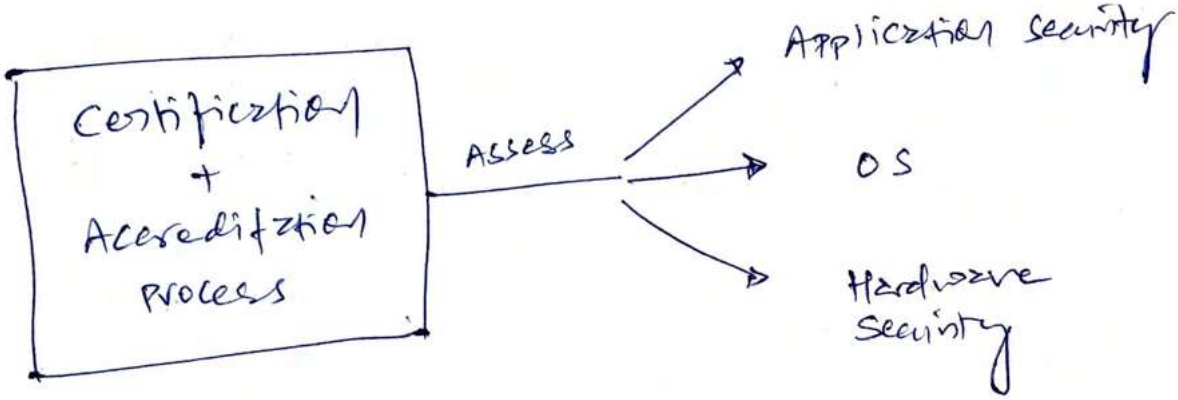
CERTIFICATION & ACCREDITATION

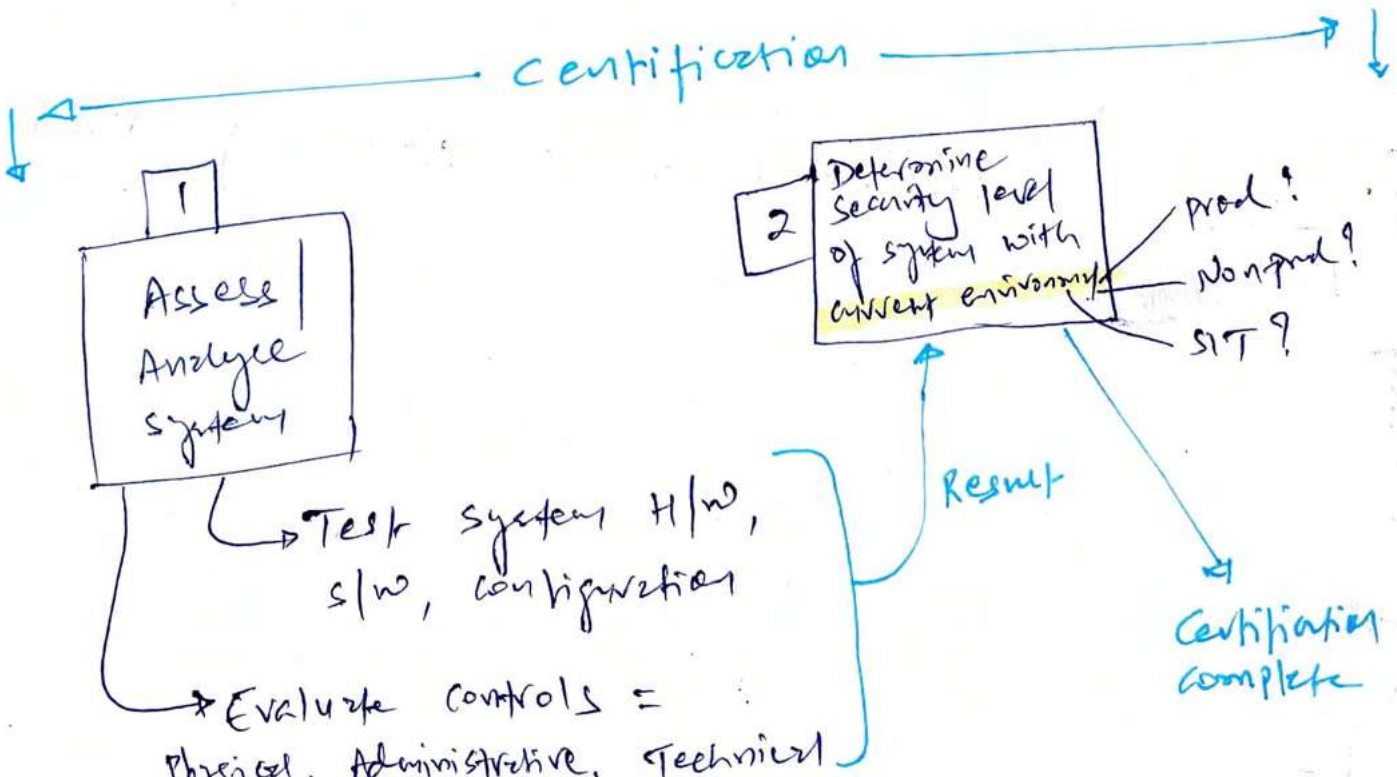
Certification: Nontechnical + Technical evaluation of system that adhers to secure design + security standards (requirements)

Accreditation: Formal acceptance of certified configuration from designated authority.

CISSP Candidate must know?

- Know the need for 'C' CERT. & 'A' Acc.
- Know which criteria are required in each phase to evaluate the system.





Certification = Valid

If → Environment
→ configuration
= same

If Environment, config = change

↳ Certification = Invalid.

Accreditation

Manage review certification

If meets organization security needs

DAA = Accreditation

- Security policy
- Security requirements
- System capabilities

Certification = Accepted by DAA

Designated Approving Authority.

RMF defines DAA as Authorization official (CAO) for Internal accreditation

+ Security control Assessor (SCA) for External Accreditation

Imp for CISSP Exam

PERSPECTIVE

Verification process is similar to certification, it goes steps beyond with involving 3rd party testing & service

NOTE:-

Also about evaluation of security controls

Certification

For

Internal verification trusted by

your → Organization

Accreditation

For

Performed by 3rd party trusted by

Everyone → WORLD

A sound security policy defines time period for valid certification & when to recertify.

P.t.o End for types of accreditation

2 standards for CERT + ACCR.

RMF
(Risk Mgmt Framework)

CNSSP
Committee on National security system (CNSS) policy

Both divided into 4 phases

Phase 1 Definition	Phase 2 Verification	Phase 3 Validation	Phase 4 Post Accreditation
Creation of System Security Authorization Agreement (SSAA)	Refine SSAA	Further refinement of SSAA + DAA recommendation + development	Maintenance of SSAA

↳ Drives entire CERT + ACCR process

UNDERSTAND SECURITY CAPABILITIES OF INFORMATION SYSTEM.

Memory Protection

is used to prevent active process from interfering with area of memory that is not assigned or allocated.

ch:9

- isolation, virtual memory, segmentation, memory mgmt, protection rings

Virtualization

- Allows any OS / multiple OS to work simultaneously on the same hardware

TPM (Trusted platform module)

TPM chip → store & process cryptographic key for Hardware encryption

More secure than software-only implementation of hard-drive encryption

HSM - Hardware Security module

- TPM is example of HSM

TPM - once harddrive is encrypted with userpass & if someone steals drive & password, they still can't decrypt it. It needs original TPM for decryption.

Bcoz

Fault Tolerance

- Critical element of secure design = redundancy
  - ch:18 (DRP)

Interfaces

(Restricted)

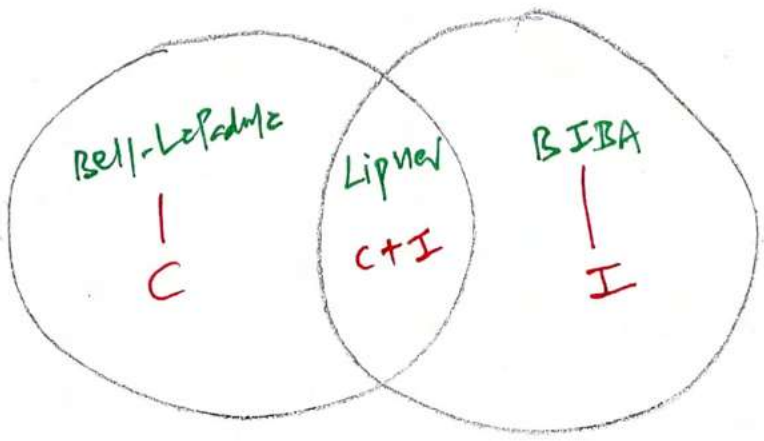
- Constrained interface = to restrict actions of authorised & unauthorised users
- Practical implementation of clark-wilson model of security.

Mindmaps notes

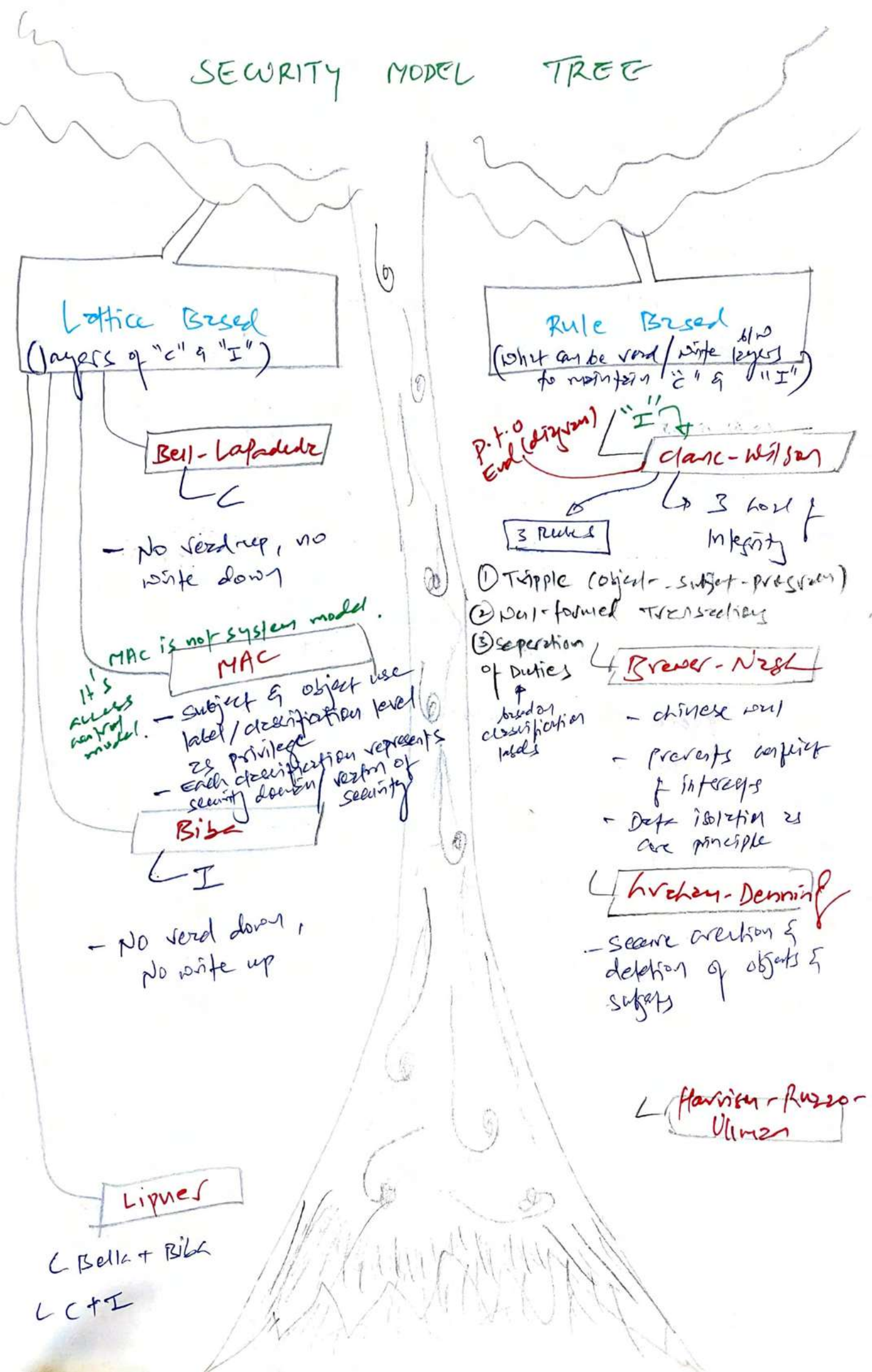
Bell-LaPadula — C	Biba — I
- Protects from low to high No Read ↑ Read ↓ simple security write ↑ No write down ↓ star - For military / federal	Read ↑ No Read ↓ simple Integrity No write ↑ write ↓ star - For commercial Applications

3 goals of Integrity

1. Prevent Unauthorised subject making ANY changes.
2. Prevent Authorised subject making BAD changes
3. Maintain system consistency



SECURITY MODEL TREE



Common Criteria Evaluation Process

identifies Security requirements for devices (class of devices) — PP (Protection Profile) — Database, FW, OS, Biometric

defines specific product from vendor that will be evaluated — ToE (Target of Evaluation) — FW: Cisco ASA

Vendor Document that claims what's in-built in the product — ST (Security Targets)

Independent lab perform test on

Security Functional Requirements

Security Assurance Requirements

Is the system provide better system security?

Are we sure it is able to provide necessary amount of security.

EVALUATE

Assign EAL — Evaluation Assurance Level

Between 1 to 7 (P.T.O)

Memorize common criteria

EAL levels

lowest

EAL 1 — Functionally tested

EAL 2 — Structurally tested

EAL 3 — Methodically tested & checked

EAL 4 — Methodically designed, tested & Reviewed

EAL 5 — Semi Formally designed & tested

EAL 6 — Semi Formally verified, designed & tested

EAL 7 — Formally verified, design & tested

highest

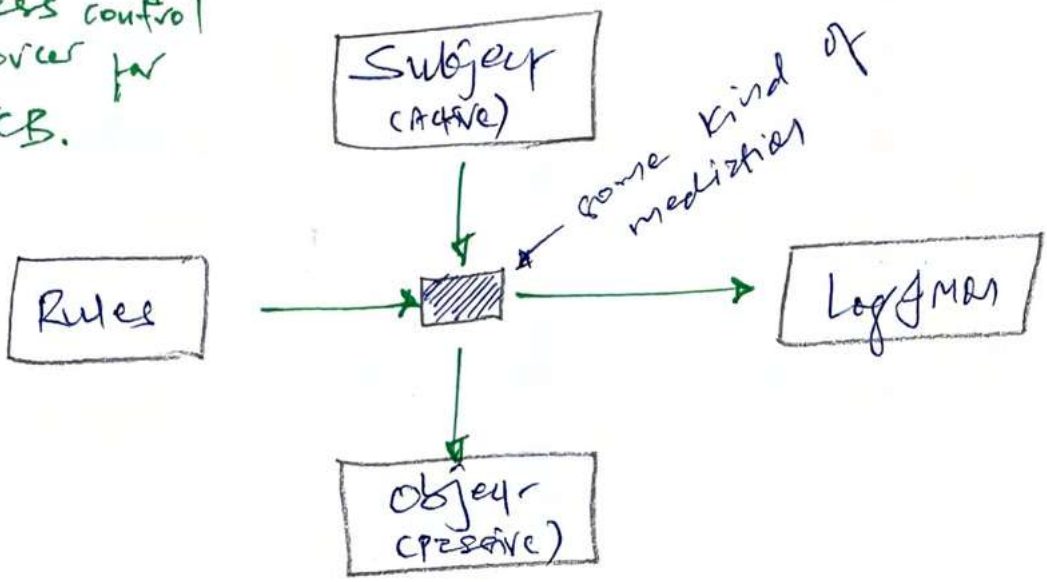
Higher EAL means not more secure, it means it's more stringently tested

MAC one or more

- Every subject & object has pre-defined ~~levels~~ lables. Based on the access, System will provide access.
- Eg. Users with "veg" lable also need another label for "lables" as data is stored in compartments. Need-to-know as being "veg", you can't have access to all veg options!!

Reference Monitor Concept (RMC)

Access control enforcer for TCB.



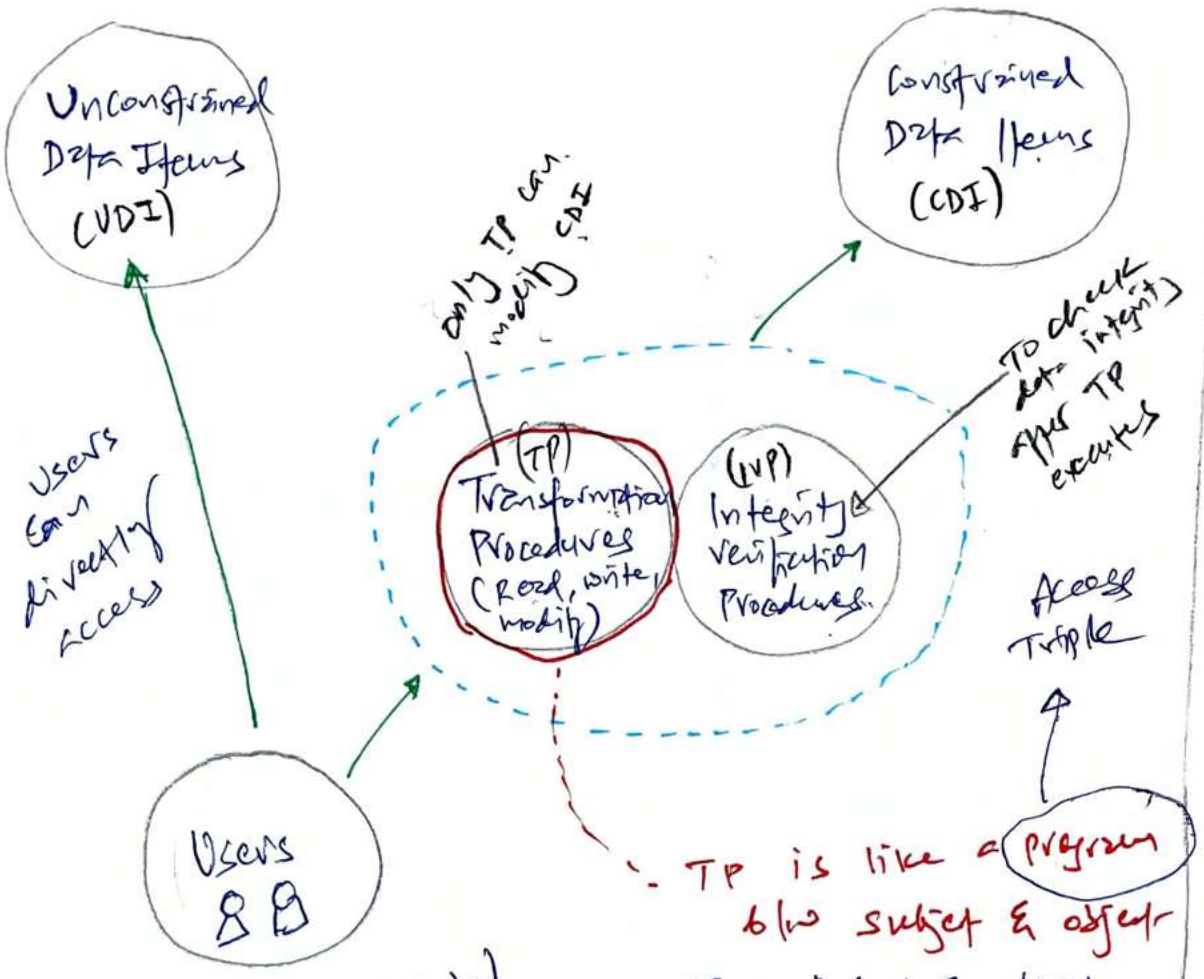
Implementation of RMC = SECURITY KERNEL

we use this to control how ~~of~~ subject will access to objects.

For RMC + security kernel, must satisfy three principles

- completeness: subject should never bypass mediation such as backdoor
- Isolation: Rules are tamperproof, only authorised can change it
- Verifiability: logging mon. to ensure mediation is working properly.

clark - wilson model



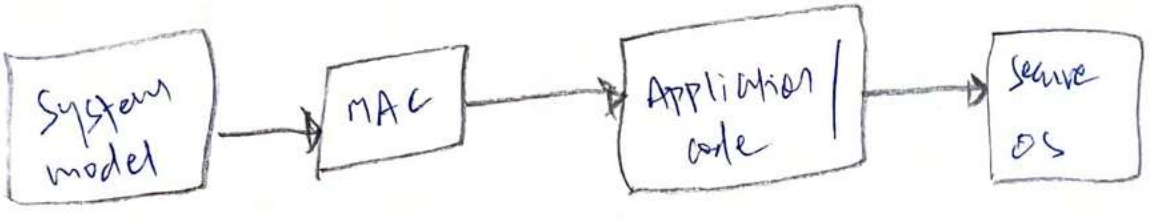
Biba Model (integrity)

write
Star Integrity → A subject can't write to files of higher integrity level.

Read
Simple Integrity → A subject can't read files from lower integrity level.

Invocation Property → A subject can't invocate data, files or service from higher integrity

Right picture



3 Types of Accredition

System accredition

- System / application evaluation

site accredition

- App / system specific, self-contained location

type accredition

- App / system that is distributed to number of different locations to be evaluated.

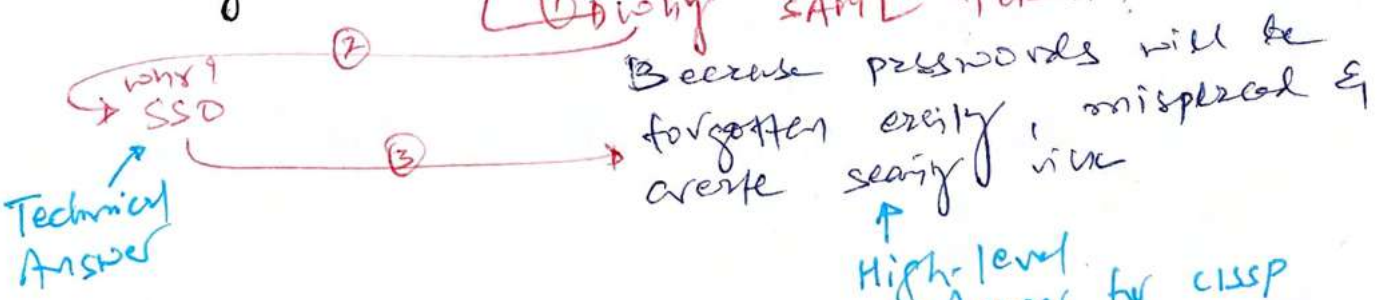
CISSP MINDSET: THINK LIKE A MANAGER

↳ Which process / systems / solution is best / fastest / most secure?

↳ Don't fix the issue. Know the process.
  ↳ Don't pick the technical answers.

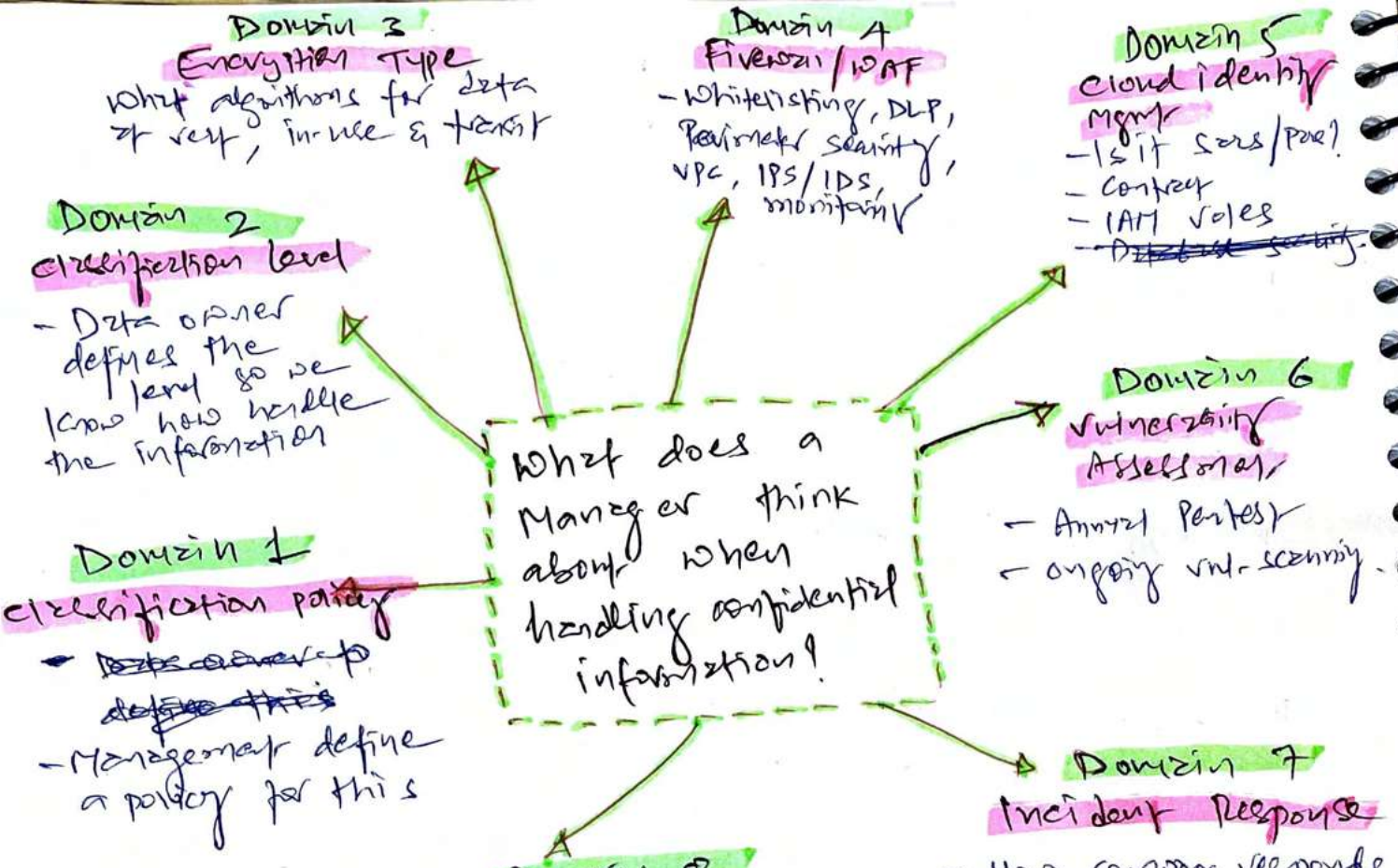
↳ Save Money. Save Human life.
  ↑ But first,

↳ Ask WHY multiple times to reach to high-level answer.



↳ Every Domains are connected with each other. Everything connects with everything in CISSP.
  ↳ All 8 domains: see it as one Fluid Entity.

P.T.O
To understand the CISSP universe.



Domain 1
Classification policy
- ~~Data owner decides this~~
- Management define a policy for this

Domain 2
Classification level
- Data owner defines the level so we know how handle the information

Domain 3
Encryption Type
What algorithms for data at rest, in use & transit

Domain 4
Firewall / WAF
- Whitelisting, DLP, Perimeter security, VPC, IPS/IDS, monitoring

Domain 5
Cloud identity Mgmt
- Is it SaaS/PaaS?
- Context
- IAM roles
- ~~Database security~~

Domain 6
Vulnerability Assessment
- Annual Pentest
- ongoing vul. scanning.

Domain 7
Incident Response
- How company responds if there is a data breach.
- What will be the process or ownership if dealing with 3rd party cloud providers
- What's the incident response plan?

Domain 8
Database Security
- what kind of access control in place for secure data?
- consider data at rest encryption.

CISSP EXAM IS NOT BASED ON WHAT YOU DO IN THE REAL WORLD.
INSTEAD, IT IS BASED ON 2 PREMISES:

1. THINK LIKE A MANAGER →
2. APPLY BEST PRACTISE →

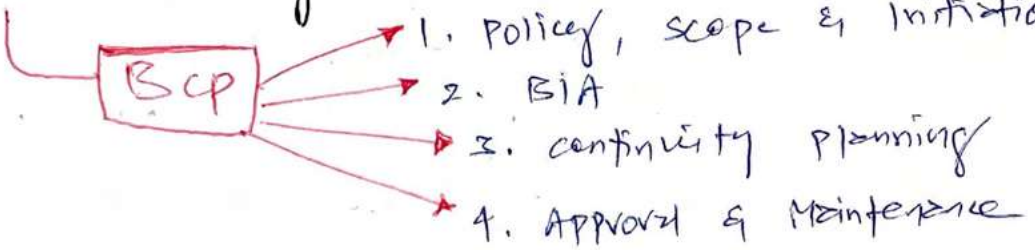
→ MITIGATE RISK

What to memorize? PRIMARY CONCEPTS IN ORDER
- Don't understand it.

(1) Human safety is the top priority. Business later.

(2) Behave ethically ——— $(ISC)^2$ code of Ethics
(laws vs. Boss)

(3) Business continuity — Business should never fail



(4) Maximize corporate benefit.

(5) Avoid or minimize threats.
Learn why, when & how to accept, reject, transfer, mitigate or avoid risk.
(Risk never disappears. It can be only reduced.)

(6) All controls must be cost justified (Safeguard)
Don't spend $100k on controls to protect $10K Asset.

(7) Security mgmt must drive security program. (top-bottom approach)

→ for CISSP Exam, pretend to be consultant for 3 yrs. Advise. Don't touch anything.

(8) Security professionals has no decision making authority.

(9) Use automated tools where appropriate

MONEY

~~Funds~~ → Understand the difference b/w cost & value

What does it mean to be GDPR ready?

With GDPR context

Firewall cost = $5K

Firewall that protect sensitive data, value = $100K

→ cost of GDPR compliance = $10K for $100K loss in revenue if not GDPR is no client wants to do business. And it cost $1M if there is a breach without GDPR.

CISSP CORE CONCEPT

if there is no process, there is no solution. (DR/BCP)

(Input to BIA) what's the role's responsibility for this process?

(Mgmt) which roles are assigned to this process?

KNOW THESE PROCESSES

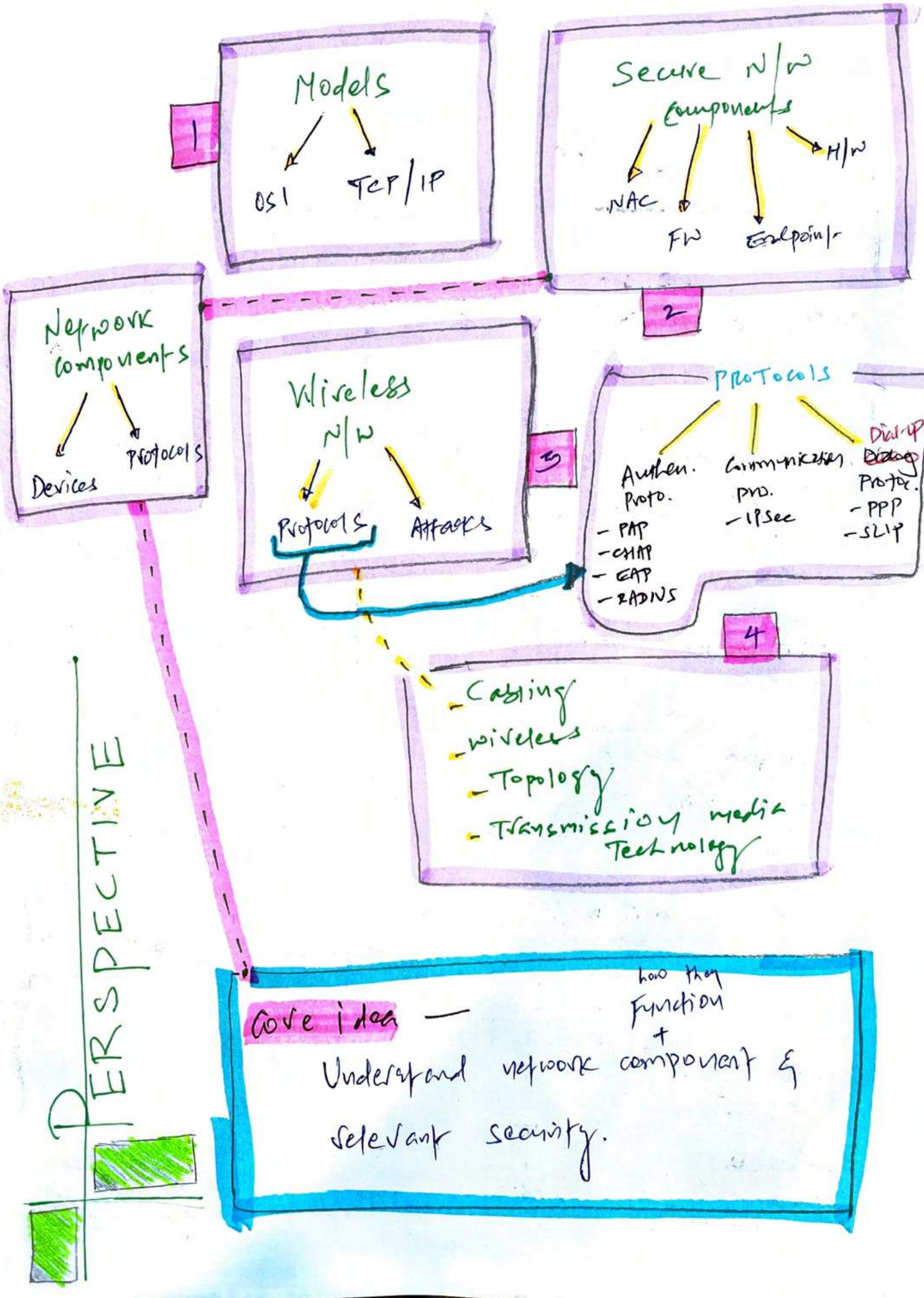
- PKI
- Incident Mgmt
- eDiscovery
- change control
- Forensic Investigation
- *BCP/DR
- Info. security Program
- RMF
- *SDLC
- Info. Lifecycle

How much technical knowledge I need for CISSP?

Do I Need to be technical? (Domain 4). N/w security.

- IPSec
- SAML
- OAuth
- SSO
- SPML
- WEP / WPA2
- Switching (broadcast + collision domain).
- TCP (3-way handshake).
- Federated Identity
- 802.1X (layer 2 technology).
- Kerberos
- OSI Model (Heart of Everything)

11. SECURING NETWORK ARCHITECTURE & SECURING NETWORK COMPONENTS



✱ OSI Model

Benefit

It's an expression of how networking actually functions.

CRITICAL

↳ Layer 7 is application & Layer 1 is physical

↳ Data streams associated with layer 7, 6, 5, from layer 4 they become segment, then packet - frame - ...

Application (7)

HTTP, FTP, LPD, SMTP, Telnet, EDI, TFTP, POP3, IMAP, SNMP, NNTP, S-RPC, SET

Presentation (6)

- Encryption & compressions
- Acts as interface b/w Network & Application
- Format types: JPEG, MPEG, ASCII, TIFF, EBCDIC, MIDI

(5) Session — comms mngmt.

- NFS, SQL, RPC
- simplex / full & half-duplex
- Retransmission failed PDUs

Transport (4)

- Integrity of connection & controlling session
- TCP, UDP, SSL, TLS, SPX

Network (3)

- ICMP, RIP, OSPF, BGP, IGMP, IP, IPSec, IPX, NAT, SKIP

(2) MAC LLC — Datalink = Ethernet

SLIP, PPP, ARP, L2F, L2TP, PPTP, ISDN

Physical (1)

EIA/TIA-232	X.21	V.24
EIA/TIA-449	HSSI	V.35

SONET

PDU - protocol data unit

Segment - TCP
Datagram - UDP

Packet

Frame

Bits

TCP/IP Model

Application

+ NFS + Windows

Transport

- host to host layer

TCP, UDP

Internet

IP, ICMP, IGMP

Link

Ethernet FDDI

Fast Ethernet

Token Ring

Routing protocols

- Distance Vector
  - RIP
  - IGRP
  - EIGRP
- Link-state
  - OSPF
  - IS-IS

MAC = H/W Address

6 Byte / 48-bit binary address

00-13-02-1F-81-53

- 3 byte / 24 bits → Vendor of physical network interface (OUI) / organizationally unique identifier
- Unique number assigned to interface by mfg.

ARP

- Resolves IP to MAC
- Dependent on Ethernet's source & destination MAC
- not true layer 2 or 3 protocol → 2.5?

TCP/IP - How to use securely?

- P.f.o TCP Vulnerability

VPN

- For C, I & Authentication
- To establish VPN
  - PPTP
  - L2TP
  - IPSec
  - SSH
  - Open VPN (SSL/TLS)

TCP wrappers

- Port based Access control
- Port based Access Control
- An application that can serve as a basic firewall by restricting access to ports and resources based on user or system ID.

TRANSPORT LAYER PROTOCOLS < TCP / UDP

IP Address + Port = Socket

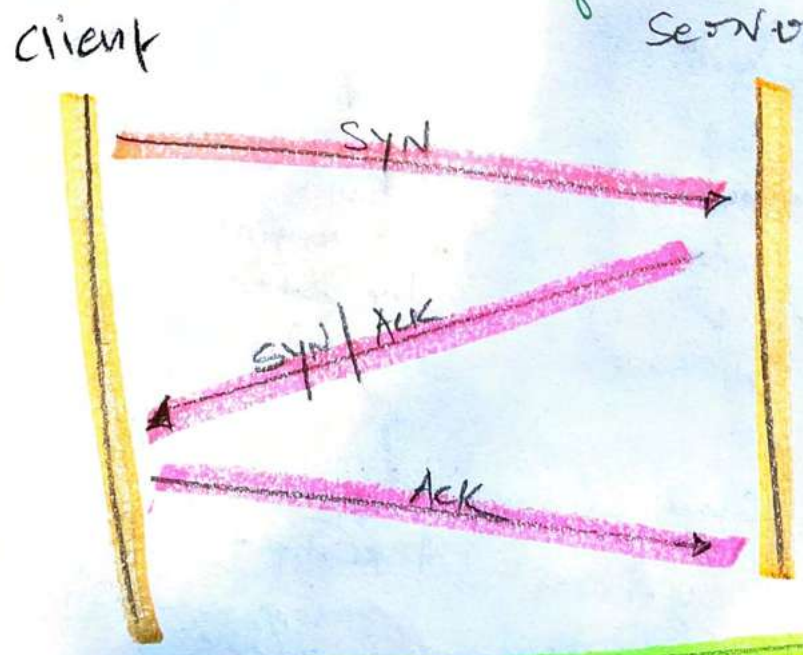
0-1023 = well known ports (service)

1024-49151
Registered s/w ports] - For client attempting to connect to their products

49152-65535
Random / dynamic / ephemeral ports / private ports

- used randomly - temporarily by client as a source port.

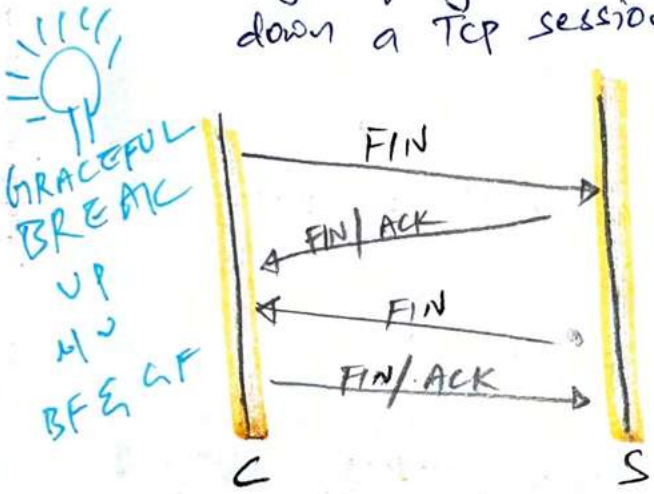
TCP 3-way Handshake For Establishing new connection



2 methods to disconnect TCP SESSIONS

FIN (finish) flagged packet

Takes exchange of four packets for gracefully tear down a TCP session



TP
GRACEFUL BREAK UP
M J
BF & GF

RST (reset) flagged packet

cause immediate and abrupt session termination

IP header protocol field value for UDP is 17

IP header protocol field value for TCP is 6

TCP concepts

Transmission window

- Number of packets transmitted before acknowledgement packet is sent

Sliding window

- To control the data flow

~~Stop~~ Small window = Use when conn is unreliable

Large window = Faster data transmission = Use when connection is reliable

REMEMBER FOR EXAM

TCP Header Flags

PSH
- Need to push data immediately to application

RST
- Reset: cause immediate disconnect of TCP session

CWR / ECE
- Explicit congestion notification
- Congestion window reduced — to manage transmission over congested links

SYN
- Request synchronization with new sequence numbers.

FIN
- Request graceful shutdown of TCP session

URG
- Indicates urgent data

ACK
- Acknowledges synchronization or shutdown requests

TCP header = 6 value

UDP header = 17

UDP ---

IP also connectionless datagram service

Doesn't provide

- Reliable delivery
- Sequence no.
- Pre-establish session
- No error detection / correction
- No flow control

Employ TCP on IP for reliability & controlled communication sessions.

* IP ~~PROTOCOL SUITE~~ NETWORKING BASIC

CIDR (Classless Inter-Domain Routing)

- Can combine multiple noncontiguous sets of address into a single subnet

class C subnet 1
class C subnet 2
class C subnet 3
→ one large subnet

IP classes — 255 = x

A — 1.0.0.0 to 126.255.255.255 — 255.0.0.0 /8

B — 128.0.0.0 to ~~222~~191.x.x.x — 255.255.0.0 /16

C — 192.0.0.0 to 223.x.x.x — 255.255.255.0 /24

D — 224.0.0.0 to 239.x.x.x — Reserved for multicasting

E — 240.0.0.0 to 254.x.x.x — Experimental

127.0.0.0 ← Loopback

255.255.255.255 ← Broadcast

IPv4 — 32-bit addressing

IPv6 — 64-bit addressing.

✱ NETWORK LAYER PROTOCOLS — ICMP, IGMP

ICMP
(Internet Control Message Protocol)

Purpose
- To check remote systems online / responding / check intermediate systems to remote end & to measure performance efficiency

Utilized by
- Ping
- Traceroute
- Pathping
-

Problems
- DDoS Attack
- Bandwidth consumption
- Ping Flood
- Smurf Attack

Solution
- limit ICMP
- Block ping on FW
- limit throughput rate

Ping of Death
Sends larger Ping >65,535 bytes

Ping Flood
DoS Attack, consumes all bandwidth

Smurf Attack
Spoofing broadcast pings

- Form of distributed DDoS Attack
- Exploits vulnerabilities of → ICMP → IP

Smurf attack generates enormous amount of traffic on target network by spoofing broadcast pings.

ICMP - Important Stuff

ICMP Header Protocol field = 1

ICMP Types

0 - Echo Reply	8 - Echo request
3 - Dest. unreachable	9 - Router Advertisement
5 - Redirect	10 - Router Solicitation
	11 - Time exceeded

IGMP
(Internet Group Management Protocol)

IP Header Protocol field value

1
2

Purpose

Multicasting

Used By

- IP Hosts to register their dynamic multicast group membership.
- Connected routers to discover multicast groups.

ARP
(Address Resolution protocol)

Core operations

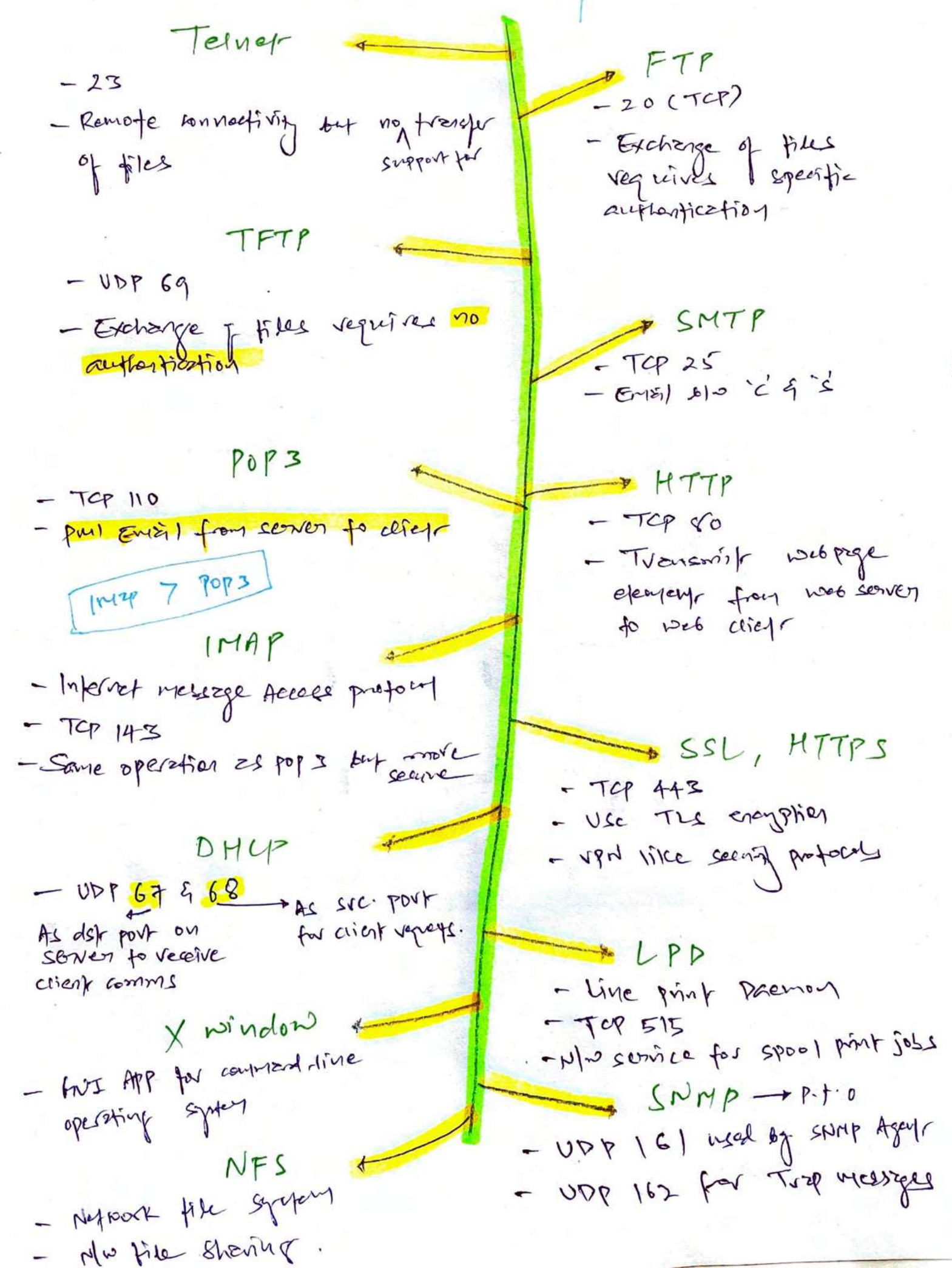
- Broadcast
- caching

Resolve IP to MAC

ARP cache poisioning

- Attackers insert bogus information in ARP cache

Common Application Layer Protocols



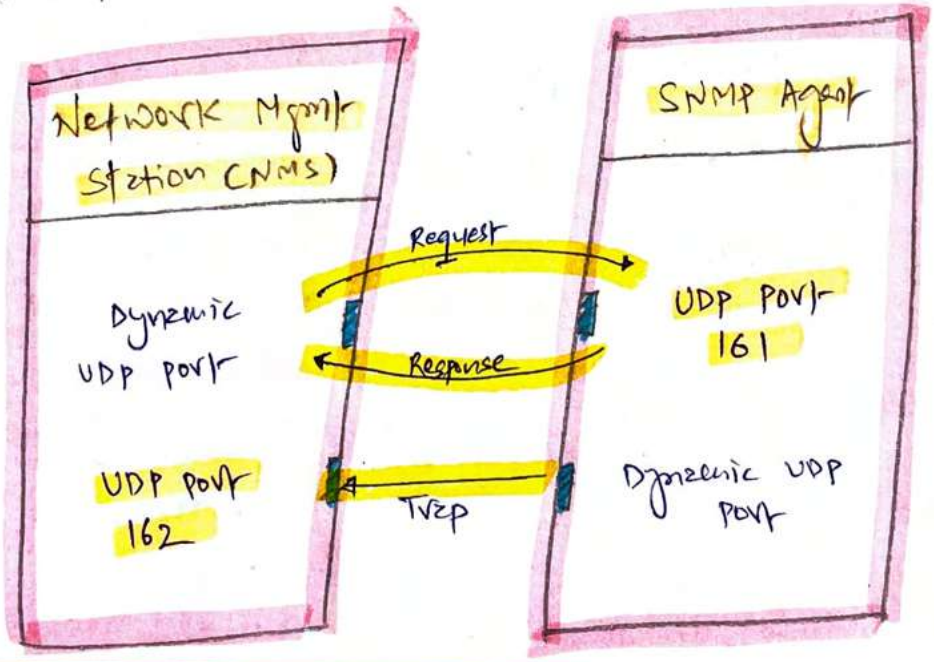
SNMP — is a network service used to collect health & status information by polling monitoring devices from a central monitoring station.

Early versions

- Plaintext transmission of community strings as authentication

latest versions

- Encrypted comms b/w device & mgmt console + Robust authentication factors



TCP/UDP, ICMP, IGMP, ARP

TCP/IP is multilayer protocol

→ there are implications (P.T.O)

Implication of multi-layer protocols

Encapsulation

Pros

- wide range of protocols can be used at higher layers
- Encryption can be incorporated into various layers
- Flexibility & resiliency in complex network structure is supported

Cons

1. Covert channels are allowed - we can hide unauthorised protocol inside authorised one

[TCP [HTTP [FTP]]]

↑ Unauthorised protocol / Not secure

2. Filters can be bypassed

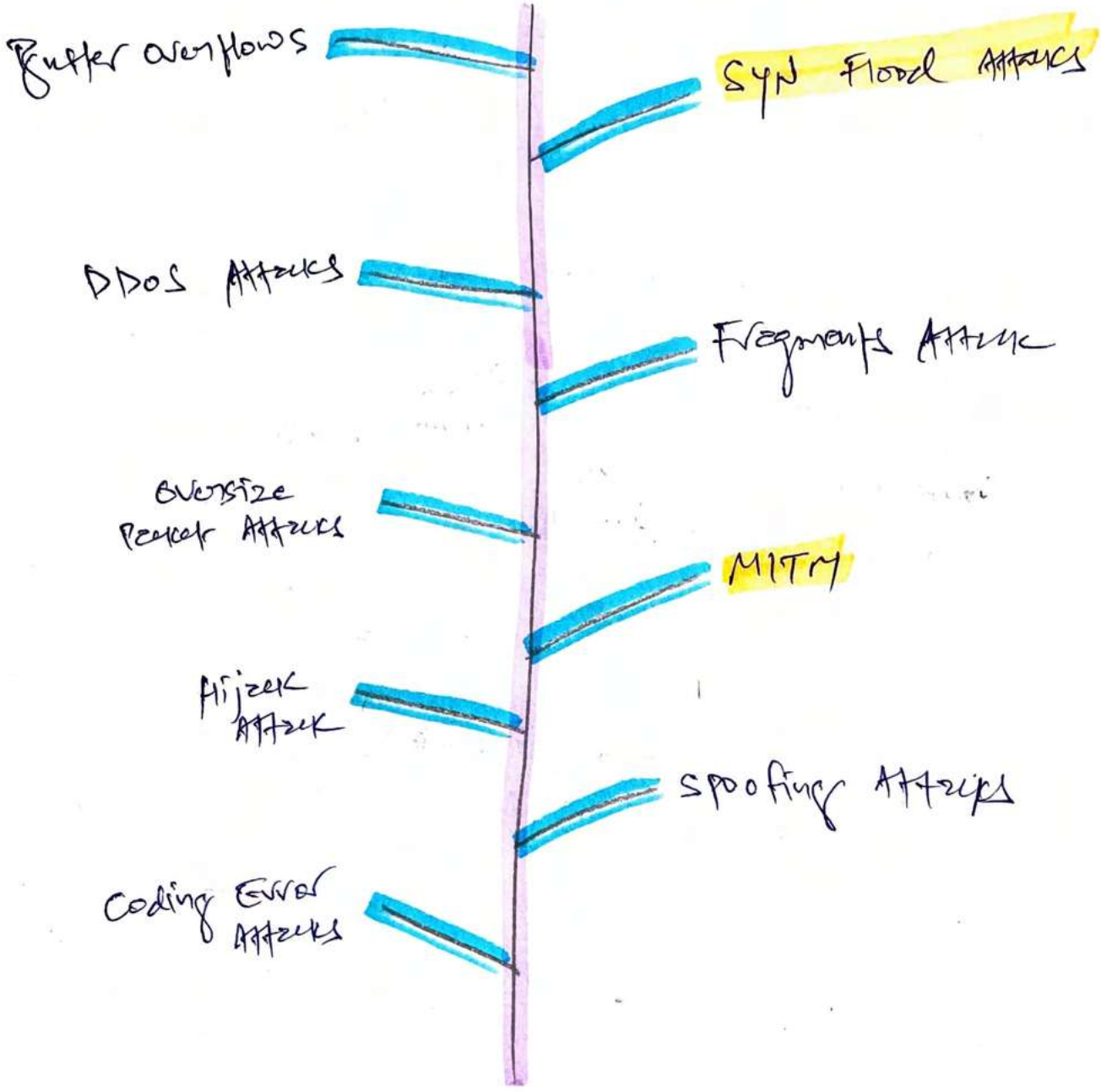
3. False Encapsulation -
E.g ICMP is only used to check health but with utilities such as LOKI, ICMP is transformed into tunnel protocol to support TCP comms.

4. logically imposed network segment boundaries can be overstepped.

5. Vlan Hopping -
Double Encapsulation where one switch remove outer tag for vlan 10 but next switch process traffic for hidden vlan 20

↑ logically imposed network segment boundaries can be overstepped.

TCP/IP Vulnerabilities



Improper TCP/IP implementation in OS is stack vulnerable to above attacks

Name to IP **DNS** → A Record

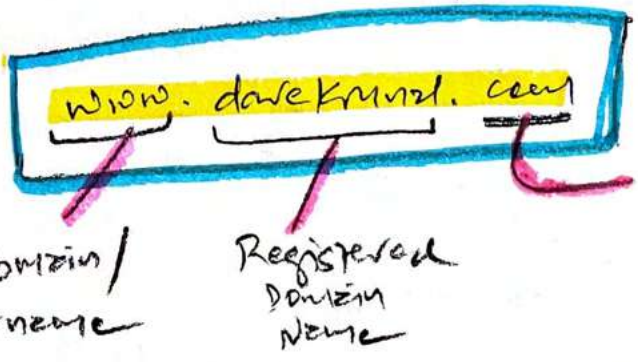
davekmuzl.com → 46.1.2.3

DNS operates over TCP & UDP 53

IP to Name **Reverse DNS** → uses PTR DNS Record

46.1.2.3 → davekmuzl.com

Need PTR Record



TLD = top level Domain

Subdomain / Hostname

Registered Domain Name

DNS Records

A
Address Record
FQDN to IPV4

AAAA
FQDN to IPV6

PTR
IP to FQDN (Reverse lookup)

SOA
Style of Authority Record
- Specifies authoritative information about zone file such as primary name server

CNAME
Canonical name
FQDN alias to another FQDN.

MX (Mail Exchange)
Mail & messaging related FQDN to IP

NS
- Authorised Name Server Record

Then: DNS was handled by static HOST file.

Now: Dynamic DNS Query (mostly for large N/W & Internet)

P.t.o more security methods

DNS security = DNSSEC

- DNS security Extensions
- Function: To provide reliable authentication b/w devices during DNS operations
- Use of Digital cert to perform mutual Auth.

DNS poisoning

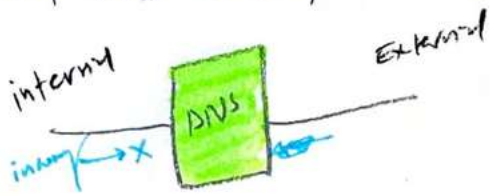
- Act of falsifying DNS information used by user to reach a desired system
- Trick → corrupt HOST file or DNS (Zone file) server query.

Other ways to Exploit DNS

- Alter HOST file
  - Putting false DNS data on client machine to redirect to false location
- Corrupt IP information
- Deploy Rogue DNS Server
  - (DNS Spoofing)
  - (DNS pharming) — modify HOST file
  - Rogue DNS server respond to client with false IP Address before real DNS server
- Use Proxy falsification
  - only for web comms
  - Attacker plants false web proxy ~~server~~ data into client browser — then modify HTTP Packets
  - Rogue proxy server
- DNS poisoning.
  - Pro Placing incorrect info. Real DNS server into zone file → send false data to servers

DNS SECURITY MEASURES

- Use DNSSEC
- Deploy NIDS
- Harden DNS server
- Limit zone transfer from internal DNS server to External DNS server



Block inbound

TCP 53 (zone transfer requests)

+

UDP 53 (queries)

Require internal clients to resolve all domains through internal DNS

Block outbound

UDP 53 (queries)

+

Keeping open outbound

TCP 53 (zone transfers)

Domain Hijacking

Sketch idea → Research Domain theft story for Fox-IT.com, sep 2017

CONVERGED PROTOCOLS

S/W-Defined Networking (SDN)

- TO FOR MORE
- seperated infra. layer from strategy to one vendor
- No concept of IP Address + subnets
- vendor neutral
- cfg. & mgmt of H/W controlled via centralized mgmt interface.

Internet Small Computer System Interface (iSCSI)

- cheaper option
- Networking storage standard based on IP
- Low cost alternative to fibre channel
- Enables location independent file storage, transmission & retrieval over LAN, WAN & Internet.

MPLS

- Directs data across network based on short Path labels rather than IP-based routing's longer network Addresses

Fibre channel over Ethernet (FCoE)

- N/W data storage / SAN operate over fibre optic cable
- Fibre channel operates on OSI Layer 2 (H/W)
- $$$$, need seperate infra (cables)

VoIP

- transport voice / video / data over TCP/IP network
- VoIP is S/W + H/W

Content Distribution Network (CDN)

= low latency + high quality throughput + high availability + high performance of hosted content

WIRELESS NETWORKS

historically insecure
- defeat insecure config from device mfg.

Data Emanation
- transmission of data across electromagnetic signals
- Hackers can re-create electron stream of magnetic field to reproduce data

802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 mbps	2.4 GHz
802.11n	200+ mbps	only 2.4 & 5 GHz
802.11ac	1 Gbps	5 GHz

* Securing Wireless Access Point

Deploy

Ad-hoc Mode
- Two wireless device with their NIC can communicate with each other without centralized control authority

Infrastructure mode
- AP is required
- Wireless NIC on system can connect directly

Four variation under Infrastructure mode

P.T.O

Infrastructure Mode

Stand-alone

AP to wireless clients but not wired

Wired-Extension

AP connects wireless clients to wired n/w

Enterprise Extended

Multiple AP connect to large physical area to serve wired n/w

Bridge

Wireless connection links two wired networks

linking n/w b/w floors or buildings

Myth Debunked – Service set identifier (SSID) is not a name of wireless network

SSID

Extended SSID (ESSID)

- Name of wireless n/w when WAP is used

Basic SSID (BSSID)

- MAC address of the Base station hosting ESSID
  - → this helps to differentiate b/w multiple base stations

* Securing SSID ----- SSIDs are broadcast by WAP via special transmission called beacon frame.

We can hide SSID broadcast but wireless sniffer can discover it.

Don't disable broadcasting SSID instead use WPA 2 instead

* Important factors for site survey

Ensure sufficient strength is available in all locations (especially in TOILET :))

Eliminate wireless signal from areas where access shouldn't be permitted (public area / outside the building)

Planning & future deployments

cyber security

SECURE ENCRYPTION PROTOCOLS

There are two methods that wireless clients can use to authenticate to WAP before normal n/w comms. can occur across the wireless link.

Open System Authentication (OSA)

- No real Authentication required
- OSA transmits everything in cleartext = NO SECURITY

Shared key Authentication (SKA)

- Some form of authentication required before comms
- WEP → WPA → WPA 2

P.T.O

WEP (Wired Equivalent Privacy)

- can crack in 60 seconds
- Provides C & I using pre-shared key
  - key used to encrypt packets before transmission
- WEP Encryption employs Rivest Cipher 4 (RC4) — symmetric stream cipher
  - RC4 does 128-bit encryption
- Poor implementation of Initialization vector (IV)
  - Refer to wireless Attacks

WPA (Wi-Fi Protected Access)

- 802.11i was developed to replace WEP.
  - defines cryptographic solutions
- Uses MIC (message integrity check) / prevents MITM + replay attacks
- Based on LEAP & TKIP = not good, crackable
- Also, use of single passphrase = downfall of WPA for Authentication

WPA 2 = for IPsec level Encryption

- Amendment known as 802.11i
- New encryption scheme - CCMP (Counter Mode cipher Block chaining Message Authentication code protocol)
  - CCMP based on AES encryption scheme → provides 256-bit encryption

2017 KRACK ATTACK

- Key Reinstallation Attack
  - Able to corrupt the initial four-way handshake b/w client & WAP into reusing previously used key

802.1X / EAP

Port-based Access control

- Client can't communicate with resource until proper authentication has take place

Extensible Authentication Protocol

- Not authentication mechanism but framework

EAP allows authentication technology to be compatible with existing wireless or P-2-P connections.

EAP-TLS
EAP-MD5
EAP Chaining

PEAP

- Protected EAP
- Usually EAP is not encrypted. PEAP can provide encryption for EAP methods
- Provides Authentication & Encryption

uses TLS

LEAP

- Lightweight EAP
- Cisco prop. to TKIP for WPA
- Avoid LEAP, use EAP-TLS

Vulnerable to ASLEAP ATTACK

MAC Filter

→ Used by WAP to block access to non-authorised devices.

- MAB (MAC Authentication Bypass)

TKIP

TKIP improvement included key-mixing function that combines initialization vector (IV) with secret root key before using that key with RC4 to perform encryption.

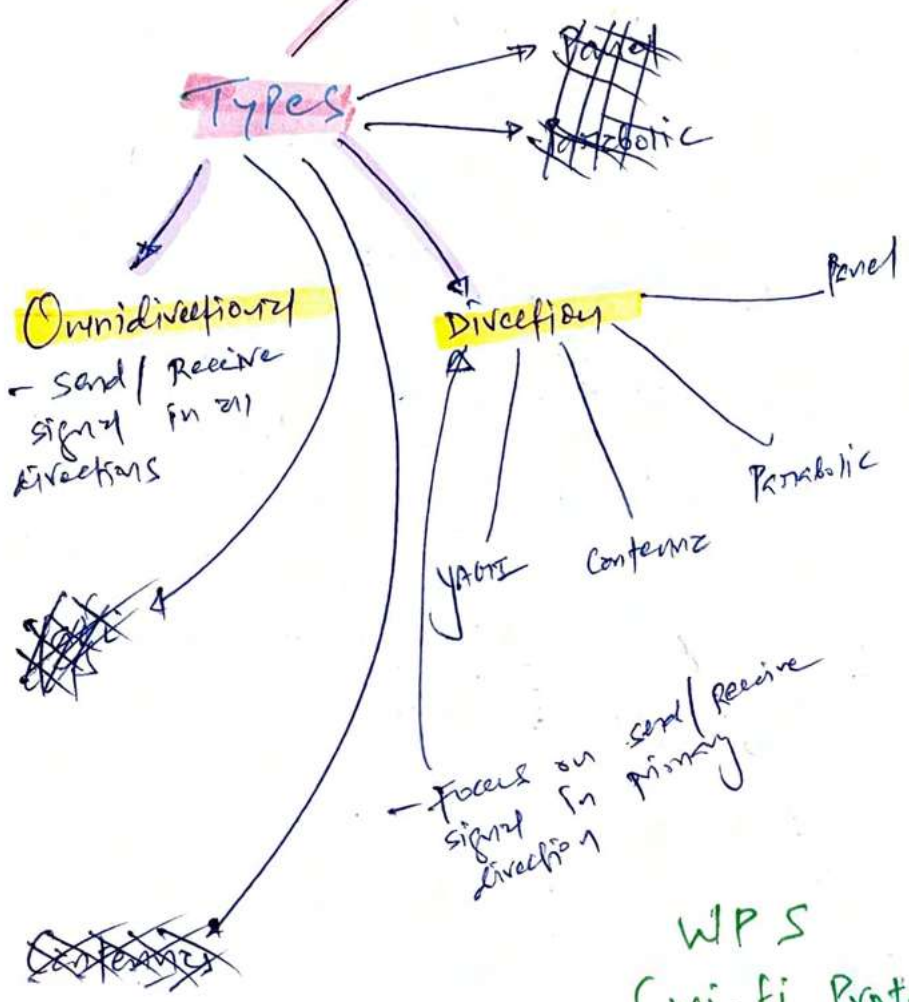
- Temporal Key Integrity Protocol
- Replacement of WEP
- Used with WPA but replaced by WPA2

CCMP

used by WPA2

- Uses AES with 128-bit key.
- No attack as yet.
- Created to replace WEP and TKIP / WPA

ANTENNA



Power levels

- Do it minor adjustment if wireless signals are not good after site survey & adjusting antenna
- Sometimes lowering Power level can enhance the performance

WPS
(wi-fi Protected setup)

- Security standard for wireless n/ws
- Simplifies effort for adding new clients to secured n/w
- Either press WPS button or call PIN (code) to trigger WPS remotely
- Leave it off unless you have to add numerous clients to wi-fi n/w

Wireless Attacks

War Driving

- Use of dedicated handheld detector (PED - Personal Electronic Device) to break wi-fi network
- Kind of performing malicious site survey for unauthorised purpose.

War chalking

- Thief that make circle in dog on selected house

- → closed / secure n/w
- ( ) → open n/w
- It's faded.

Replay

- Focus: initial Authentication Abuse
- Retransmission of captured comms to gain access to target system
- Mitigation: Updated firmware of base station + W-IDS / W-NIDS

Recommended reply includes base stations MAC Address + SSID

IV (Initialization Vector)

- WEP's primary weakness = poor implementation IV
- IV is a cryptographic random number
- IV is based on RC4

WEP IV is only 24bit long & transmitted in plaintext

Rogue AP

- Usually discovered during site survey
- Rogue WAP duplicates valid WAP's MAC, SSID, channels
- Rogue WAP = social Engg. Attack with look like SSID
- Sol: Use wireless IDS for rogue detection

Evil Twin (बहुरूपिया)

- False WAP automatically clone / twin using evasdropping when client reconnect to real WAP.
- It's a MITM Attack: session hij., data theft, credential theft
- Defense: Regularly purge old wireless profiles

Secure Network Components

Types of network traffic

- Intranet → Private
- Extranet → DMZ
- Internet → Public

Networks are segmented because ...

- Boost Performance
  - E.g. Routers divide broadcast domains
- Reduce communication problems
  - Reduce congestion such as broadcast storms
- Providing security
  - isolate traffic + user access for authorised purpose

Do segment using

- VLANs
- Routers
- switches
- Firewalls

~~CRITICAL~~

- Multihomed FW
- FW Deployment Architectures

p.f.o.

End

* Network Access Control (NAC)

Goals

- Prevent zero-day Attacks
- Enforce Security Policy throughout the network
- Use identities to perform Access control

NAC refers to an automated detection & response system that can react in real-time to stop threats as they can occur & before they cause damage or a breach

NAC = preventive, detective, corrective

NAC Implemented as

Preadmission Philosophy

- Requires systems to meet all security requirements before allowing communication with the network
  - Security Posture

Postadmission philosophy

- Allows / Denies based on predefined Authorization matrix.

* Firewalls

i) Static packet Filtering Firewall

- 1st generation, layer 3 @ OSI
- filters traffic by examining data from message header.
- No user authentication
- Rules revolve around src, dst & port

Note - firewall provide protection for traffic b/w subnet, not within subnet (no protection behind the firewall)

ii) Application-level Gateway FW

- 2nd generation, layer 7 @ OSI
- Filter traffic based on Application/ Internet Service
- A.K.a = Proxy FW → changes src & dst address to protect identity of private network
- Negatively impact performance as each packet must be examined & processed as it passed through Firewall

iii) ~~Circuit-level Gateway~~ Stateful Inspection FW

- 3rd Gen, layer 3 + 4 @ OSI
- A.K.a = Dynamic packet filtering / stateful inspection
- Evaluate state or context of network traffic such as previous packet of the same session

stateful

v) Deep Packet Inspection Fw (DPI)

- Layer 7

PAyload = deep

- filter payload content of communication along with the header values
- A.k.a = complete inspection / information extraction (IX)
- Block malware, spam, block domain names
- often integrated with App. Fw.

vi) Next-Gen Firewalls

- IPS / IDS, TLS / SSL proxy
- Antivirus
- Bandwidth throttling
- VPN Anchoring
- QoS Mangemt
- Web filtering

(iii) circuit-level Gateway Fw

- layer 5 @ OSI
- Used to establish communication session b/w trusted partners.
  (E.g SOCKS (socket secure))
- A.k.a = circuit proxy - they merge comms based on circuit, not content of traffic
- 2nd Gen

Multi / Dual-Homed Firewalls

- At least has two interfaces to filter traffic
- IP forwarding should be disabled, which automatically forward traffic from one interface to another one

Bation Host ——— screened host

- host exposed to internet with hardening
- Sacrificial host that will receive all inbound attacks
- Act as a proxy for all trusted systems within private network

Firewall Deployment Architecture

- **Single Tier**
  - Minimum protection
- **Two Tier**
  - Moderate level of routing & filtering complexity
- **Three / multi Tier**
  - Seperated by multiple subnets
  - Eg DMZ as subnet
  - Most secure
  - most complex

* Endpoint Security

The end device is responsible for its own security.

* Secure Operation of Hardware

↳ Repeaters, concentrators & Amplifiers

→ Layer 1 of OSI

↳ Hubs = same collision domain + broadcast domain

- same collision domain: Seperated by Layer 2 device
- broadcast domain: Seperated by Layer 3 device

↳ Modems = WAN technology | 1960 - 1990

Bridges — Layer 2 @ OSI

- Same broadcast domain, different collission domains
- Store-and-forward device

Switches

Layer 2 @ OSI

- One broadcast domain
- Seperate collision domain

Layer 3 @ OSI

- vlan, routing
- Seperate broadcast & seperate collission domain

Routers — layer 3 @ OSI

- Systems on either side of router are part of different broadcast & collision domain

Brouter — first attempt to route, if fails, it defaults to bridging

- layer 3 @ OSI
- Seperate broadcast + collission domains

- layer 2 @ OSI
- one broadcast + seperate collision domain

Gateways

- connects networks that use different protocols.
- A.K.a = protocol translators
- different broadcast domains + different collision domains.

Proxies

- NAT / PAT servers
- Cache servers
- Provide Internet access to private network & hide/protect identity of clients

LAN Extenders

= creates WAN! weird.

- is remote access, multi-layer switch used to connect network over WAN links.

✡ CABLING

Transmits one signal at time → Baseband and Broadband cables

Transmits multiple signals

10 BaseT

XX YYYY ZZ

- XX = maximum speed cable type offers (10)
- YYYY = baseband or broadband
- ZZ = maximum distance the cable can be used or to present technology.

Coaxial Cable

- Thinner 10Mbps → 10Base2 185 meter
- Thicker 10Mbps → 10Base5 500 meter

↳ Support high bandwidth, offers longer cable than twisted pair & fairly resistant to electromagnetic interference (EMI).

Best: lower cost + ease of installation

Conductors

- copper
- Alternate to conductor-based network cabling is Fibre optic (copper alternative) → + 2Gbps speed

Twisted pair

unshielded twisted pair (without foil)

- most common UTP: Unshielded Twisted pair
  - ↳ 10BaseT → 100 meter
  - ↳ 100BaseT
  - ↳ 1000BaseT → 1Gbps

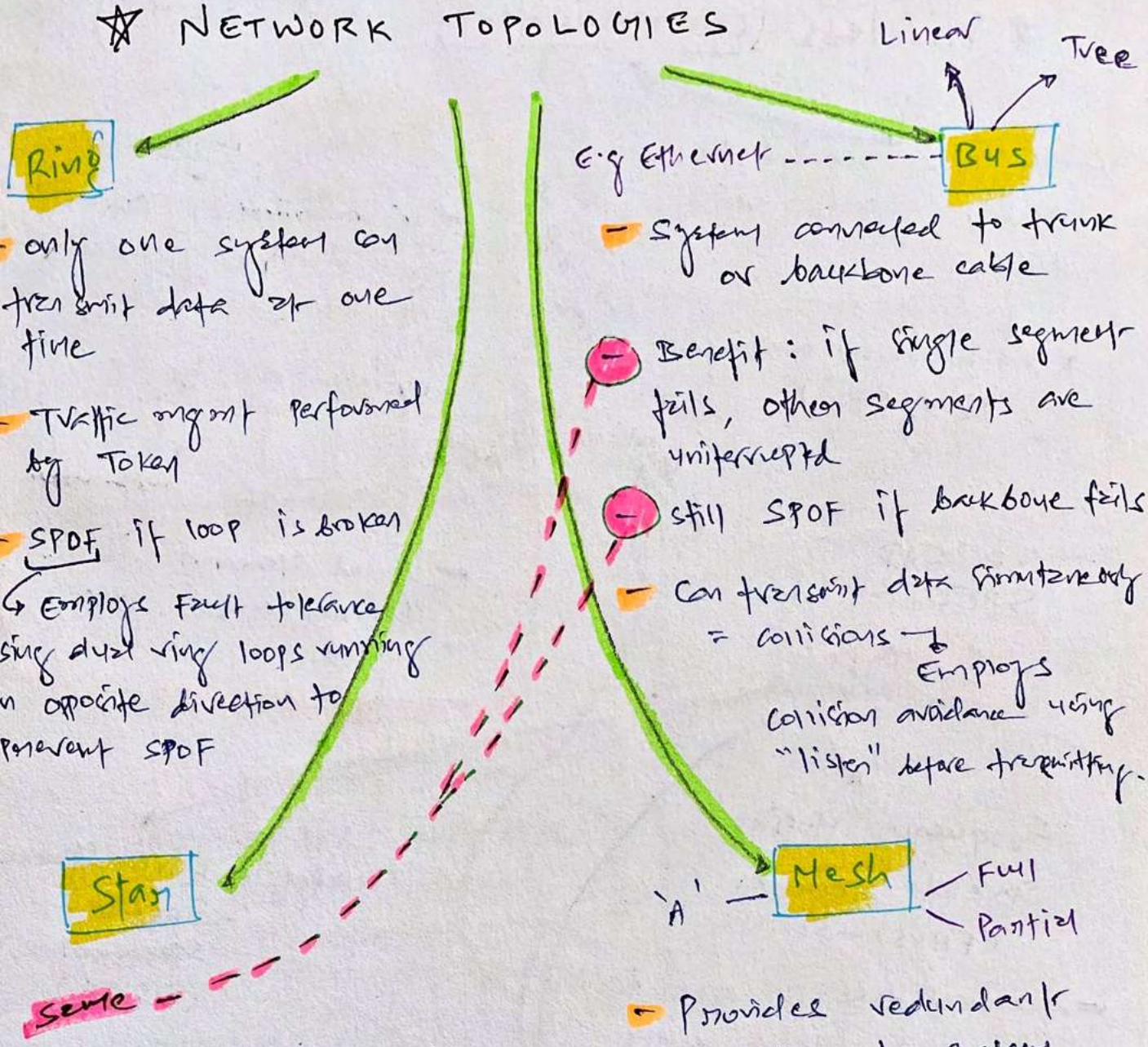
- Copper problem = Attenuation
- move speed = more Attenuation
- Solution = use shorter cable for high speed transmission.

Coaxial cable	distance	Twisted pair cable
	>	

data transmitted over one set of wire picked up by another wire due to electromagnetic field.

Tighter the twist = more resistant to internal & external interference & crosstalk, greater throughput

✡ NETWORK TOPOLOGIES



Ring

- only one system can transmit data at one time
- Traffic mgmt performed by Token
- SPOF if loop is broken
  - ↳ Employs Fault tolerance using dual ring loops running in opposite direction to prevent SPOF

Bus

- Systems connected to trunk or backbone cable
- Benefit : if single segment fails, others segments are uninterrupted
- still SPOF if backbone fails
- Can transmit data simultaneously
  - = collisions → Employs collision avoidance using "listen" before transmitting.

Star

- Centralized connection device such as switch / hub
- Logical bus and logical ring can be implemented as physical star

Mesh

- Provides redundant connections to system, allowing multiple segment failure without affecting connectivity.

Note — Gateway → only useful if network protocols are changing.

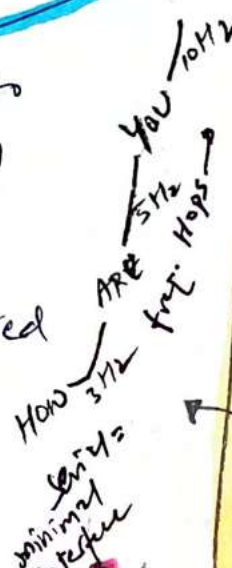
Cat 7 → Appropriate for 10 Gbps network at much shorter distance.

STP Cable → limited to 155 Mbps & 100 meters.

✱ Wireless Communications and Security

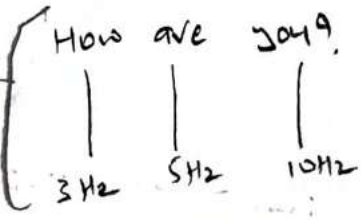
Employ radio waves to transmit signals over a distance

→ Radio spectrum measured with Hertz (Hz)



Spread Spectrum

- Communication occurs over multiple frequencies at the same time



- spread spectrum is parallel comms, not serial.

SPREAD SPECTRUM'S

3 Types

Frequency Hoping Spread spectrum (FHSS) – Serial

- transmit data in serial fashion (not parallel) while constantly changing frequencies in use
  - Also helped to minimize interference
- Entire range available but only use one frequency at a time

Direct Sequence Spread Spectrum (DSSS)

Parallel

Employs Available Frequency

- transmit data using parallel
- Occurs same way as parity of RAID-5 allows data on missing drive to reserved

Orthogonal Frequency-Division Multiplexing (OFDM)

- Employs digital multicarrier modulation scheme that allows tightly compacted transmission.
- Perpendicular modular signal = No interference with each other.

Cell phones

- Provider's tower can be simulated to conduct MITM attacks

Bluetooth

- IEEE 802.15 / Personal Area N/w (PAN)

* Attacks → Bluejacking
  - Bluesnarfing
  - Bluebugging

RFID

- Radio frequency identification
- tracking technology
- RFID Reader can collect information transmitted by activated chips in the area

NFC

- Near field comms.
- Smartphones: device to device data exchange
- Radio based tech.

* Attacks → MITM
  - Eavesdropping
  - Data Manipulation
  - Replay

Cordless phones

- Designed to use unlicensed frequencies (900 MHz, 2.4/5 GHz)
- Eavesdropping

✱ LAN Technologies

Ethernet

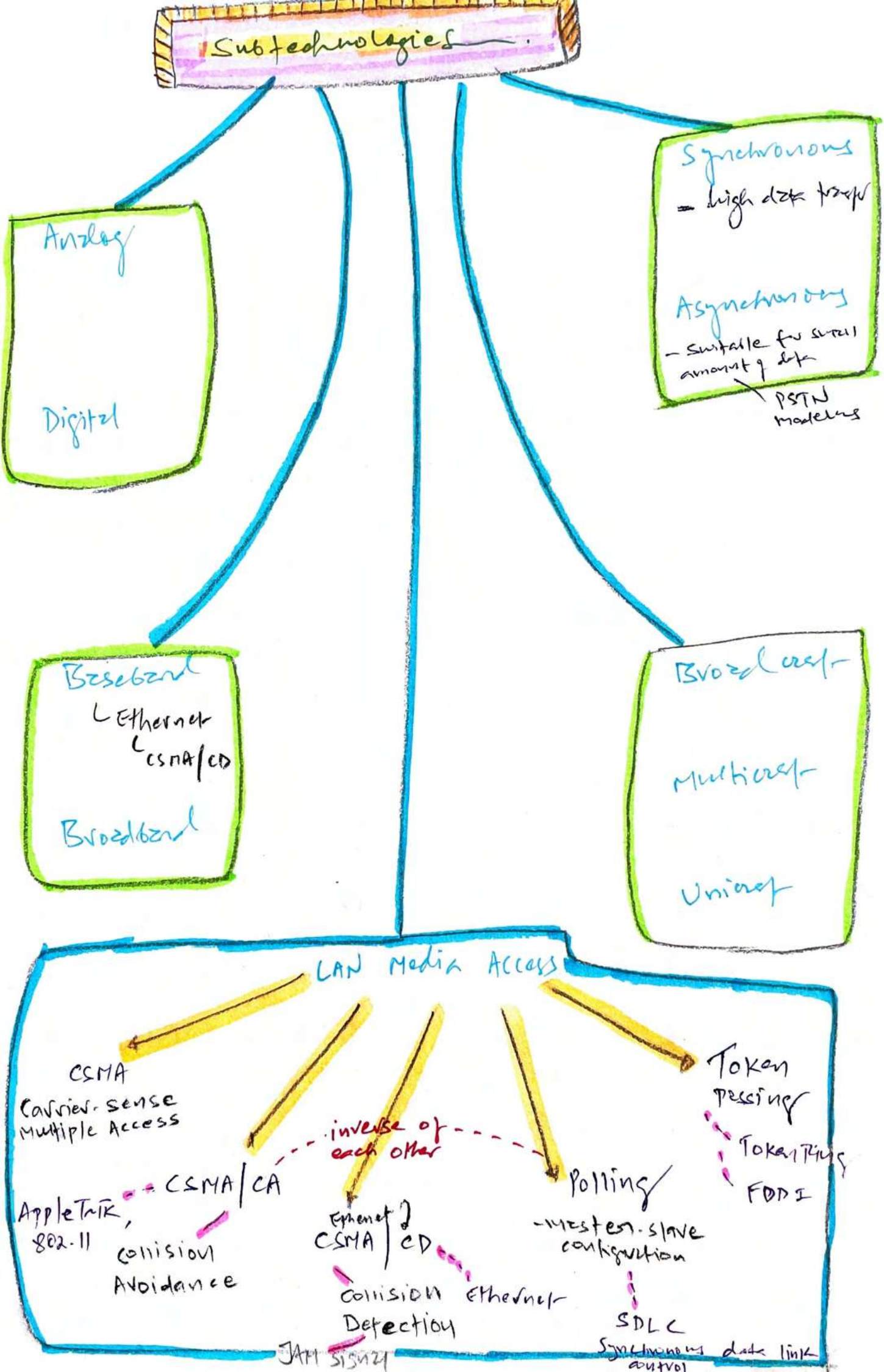
- Full-duplex, twisted-pair cabling
- Employs broadcast and collision domain
- IEEE 802.3 standard
- A.k.a: Shared-media LAN technology / broadcast technology

Token Ring

- token travels in a logical loop in LAN
- Employed in ring or star topologies.
- Deployed as physical star using Multistation Access unit (MAU)

FDDI (Fibre Distributed Data Interface)

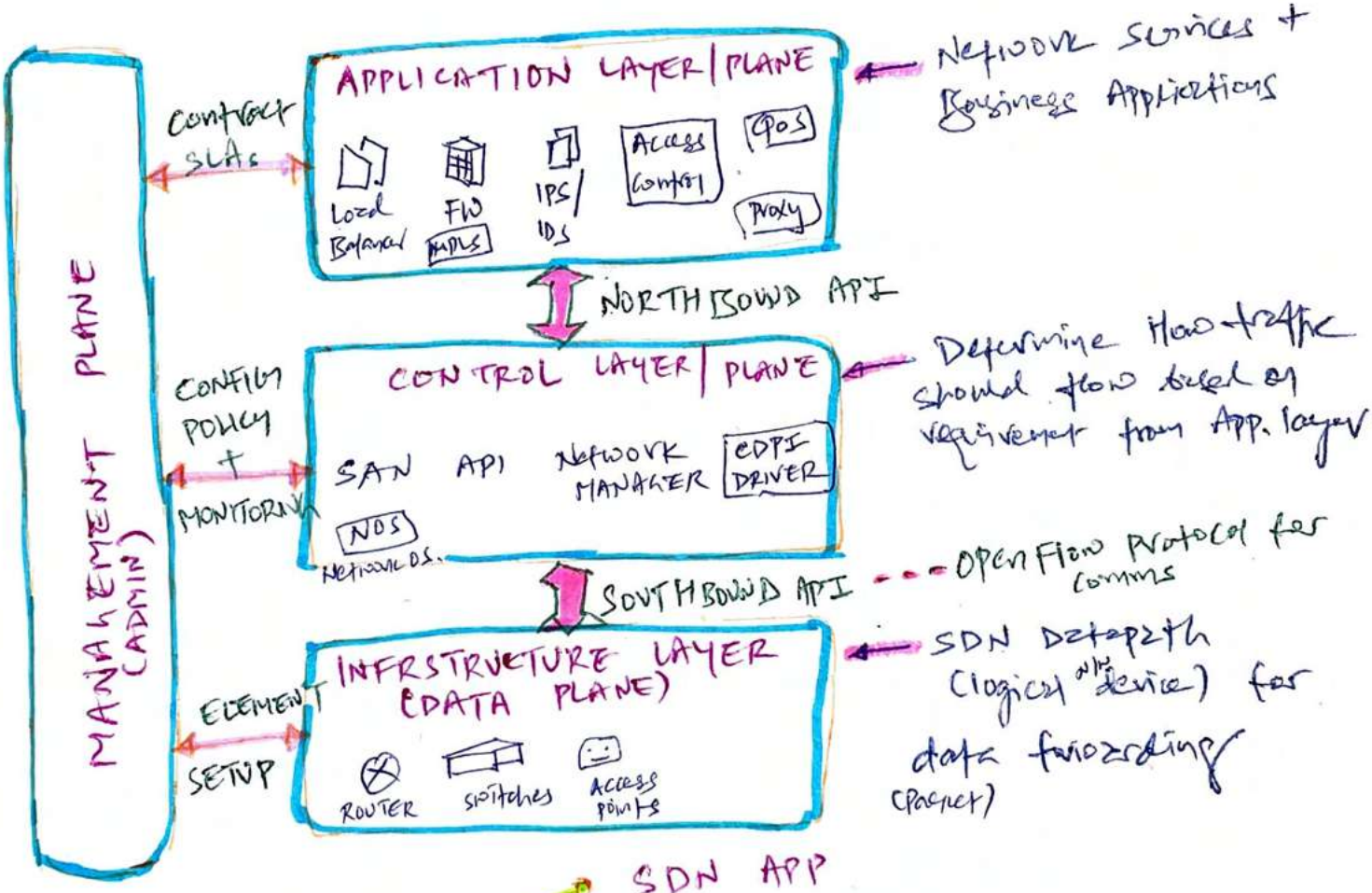
- high speed token passing technology
- $ $ $ $ $ $
- Used as backbone for large enterprises
- Dual ring design = self healing by removing failed segment
- Two rings: traffic flowing in opposite direction


Subtechnologies
Analog
Digital
Synchronous
- high data transfer
Asynchronous
- suitable for small amount of data
PSTN modems
Baseband
Ethernet
CSMA/CD
Broadband
Broadcast
Multicast
Unicast
LAN Media Access
CSMA
Carrier-sense Multiple Access
CSMA/CA
inverse of each other
Token passing
Token Ring
FDDI
AppleTalk, 802.11
Collision Avoidance
Ethernet
CSMA/CD
Collision Detection
Jam signal
Polling
-master-slave configuration
Ethernet
SDLC
Synchronous data link control

SDN - SOFTWARE DEFINED NETWORK

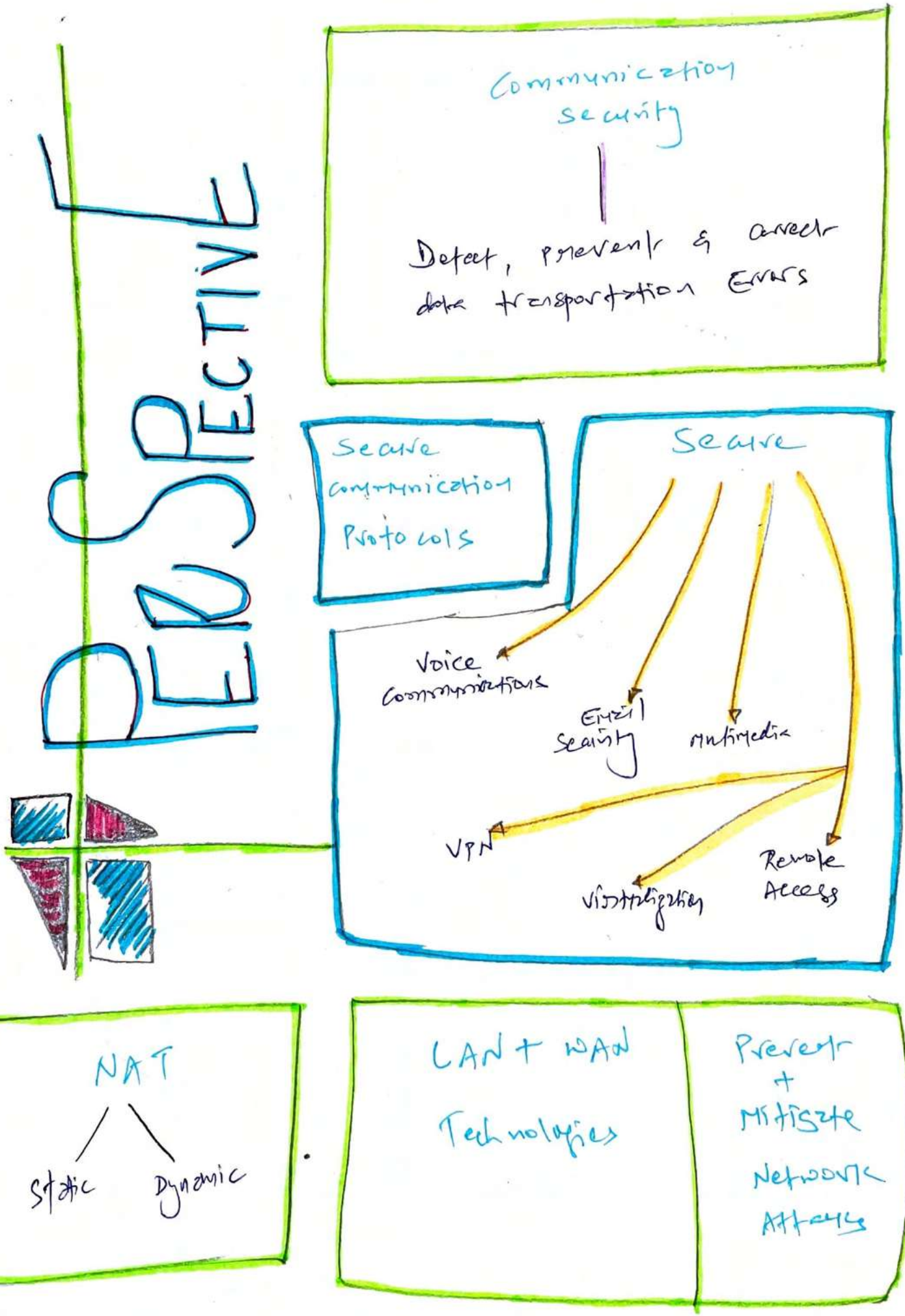
- SDN seperates routing & forwarding decisions of networking elements from Data plane

SDN Architecture
- APPLICATION PLANE
- CONTROL PLANE
- DATA PLANE



SDN CORE COMPONENTS
- SDN APP
- SDN CONTROLLER
- SDN DATAPATH
- SDN control to Data-Plane Interface (CDPI)
- NBI - NORTH BOUND INTERFACE
- SBI - SOUTHBOUND INTERFACE
- Mgmt + Admin

12. SECURE COMMUNICATIONS AND NETWORK ATTACKS



✱ Secure Communication Protocols

IPSec

- Uses PKI to provide Encryption, Non-repu. + msg auth.
- IP based protocol

(S-RPC)

Secure Remote Procedure call

- Authentication service
- Prevents unauthorised execution of code on remote system

Kerberos

- SSO
- Hybrid ~~authentication~~ Encryption + authentication protocol

SSH

- End to end Encryption

Signal Protocol

- End-to-end encryption for voice / video / messaging Apps

SSL

TLS

Secure Socket layer

- 40-bit | 128-bit key

Transport layer security

both

Prevents spoofing, tampering + eavesdropping

- Both can be implemented to lower layer (layer 3) to operate as VPN, called OpenVPN

* Authentication Protocols

~~(MORE)~~ Move on ~~BOSON~~ BOSON ~~NOTES~~ coffee

(CHAP) Challenge Handshake Auth. Pro.

- Used over point-to-point (PPP) links
- Authentication using challenge-response dialog that cannot replayed
- Periodic reauthentication of established session

Protection against Replay attacks

(PAP) Password Auth. Pro.

- Transmits username & password in clear text
- No Encryption

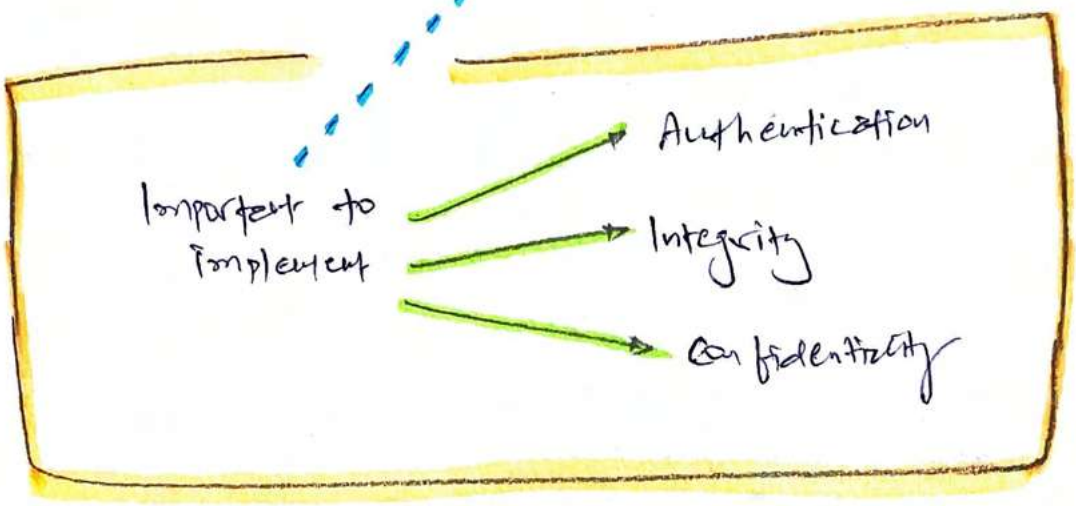
(EAP) Extensible Authentication Protocol

- This is framework of authentication instead of actual protocol

Allows customized authentication Security solutions

- EAP-TLS
- PEAP
- LEAP

* Secure Voice Communications



PBX / POTS Vunerable to + PSTN

- Eavesdropping
- Tapping
- interception

VoIP

Encapsulates Audio into IP packets to support telephone calls over TCP/IP network.

VoIP problems

- MITM
- DS + DOS Attacks
- Vishing (VoIP phishing)
  - Caller ID can be falsified
  - A.K.A = SPIT Attack (Spam over Internet Telephony)
- 802.1x Authentication falsification (vlan Hopping)
  - Risk where VoIP phone & servers are on the same switches
- VoIP traffic Unencrypted = risk

Social Engineering

Exploits human characteristics

Attackers bypass physical and logical (technical) security controls punching holes in security perimeter.

Tools p.t.o

Phreakers — They gain unauthorised access to personal mailboxes, redirect messages, block access, redirect inbound/outbound calls.

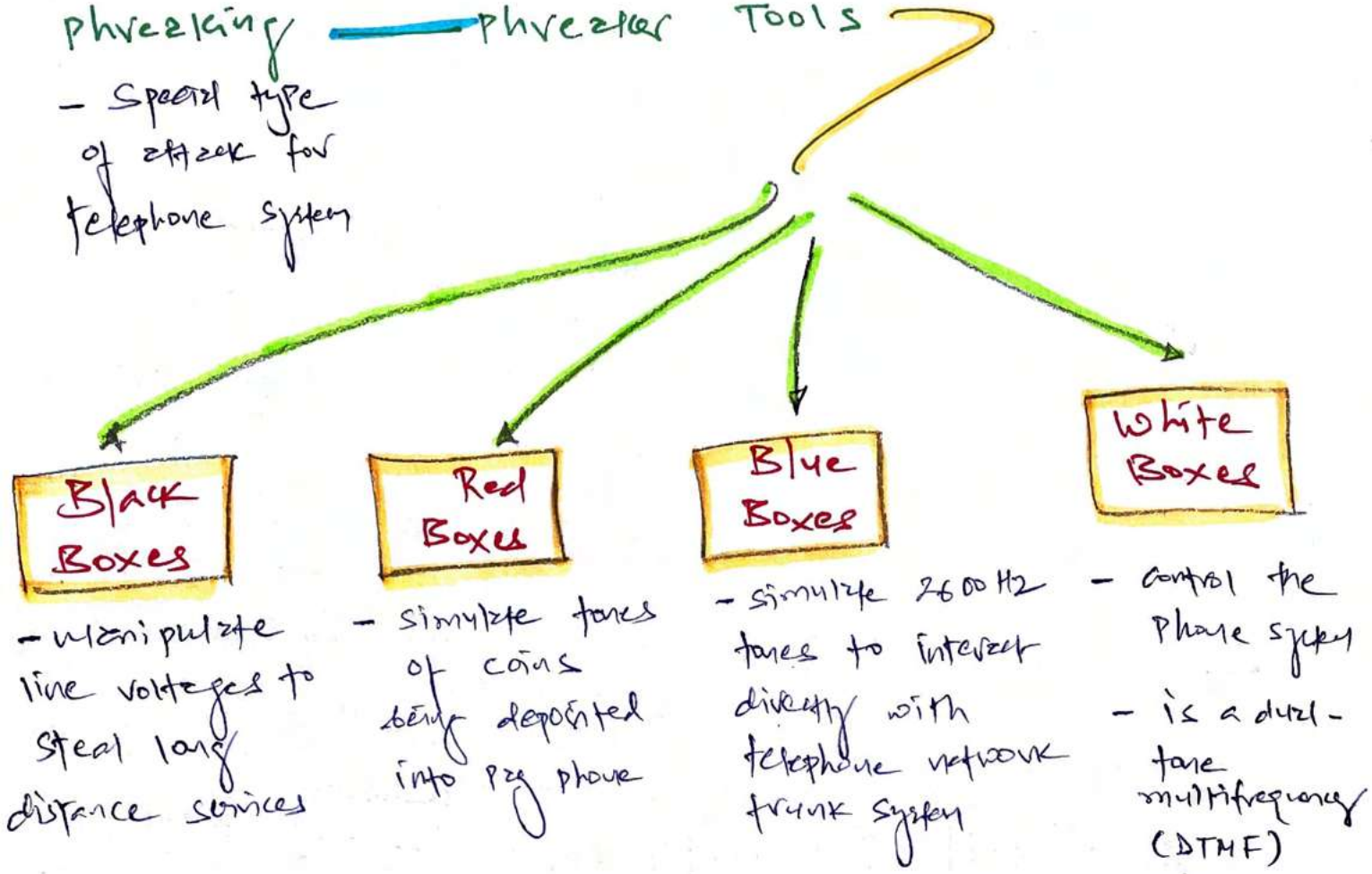
They are threat to PBX (private branch exchange)

Reduce PBX fraud with DISA (Direct Inward System access)

- DISA is designed to help manage external access and external control of PBX by assigning access codes to users.

Phreaking — Phreaker Tools

- Special type of attack for telephone system



☆ Multimedia Collaboration

- Remote Meeting
- Instant Messaging (IM)
  - susceptible to packet sniffing
  - No protection for Piracy

☆ Email Security ----- security issues (P.T.O)

- Email server – SMTP
- Email clients – POP3, IMAP

Careful! SMTP server should not turn into Open Relay
- means SMTP server doesn't authenticate senders before accepting and relaying mail

Note - Many internet-compatible Email system rely on X.400 standard for addressing and message handling.

Note - Email security begins in a security Policy approved by upper mgmt.

protocols: IMAP, POP & SMTP do not employ encryption natively.

Email Security Issues

POP3, IMAP, SMTP
= don't employ encryption natively
+
modify email in transit (integrity issue)

Delivery of trojan, virus, worms

Spoof source email = spamming

Mail Bombing (DDoS Attacks)

POP: download onwer

Email security solutions — P.T.O

P.T.O 2 type of messages

S/MIME — Security Multipurpose Internet Mail Extensions

- Auth & C to email via public key encryption and digital signatures
- Uses X.509 → P.T.O for client

MIME object Security Service (MOSS)

- Uses MD2, MD5, RSA, DES for Encryption & Authentication
- provides C, I, Auth, NP of email messages

SPF — Sender Policy Framework

- Protection against spam & email spoofing
- check inbound msg originate from authorised SMTP server.

opportunistic ~~for~~ TLS for SMTP Gateways

- Encrypted connection with every other email server
- protects from sniffing of email

Pretty Good Privacy (PGP)

- Public private key system used in IDEA

Privacy Enhanced Mail (PEM)

- Use of RSA, X.509, DES
- Provides C, I, Auth & NP

DomainKeys Identified Mail (DKIM)

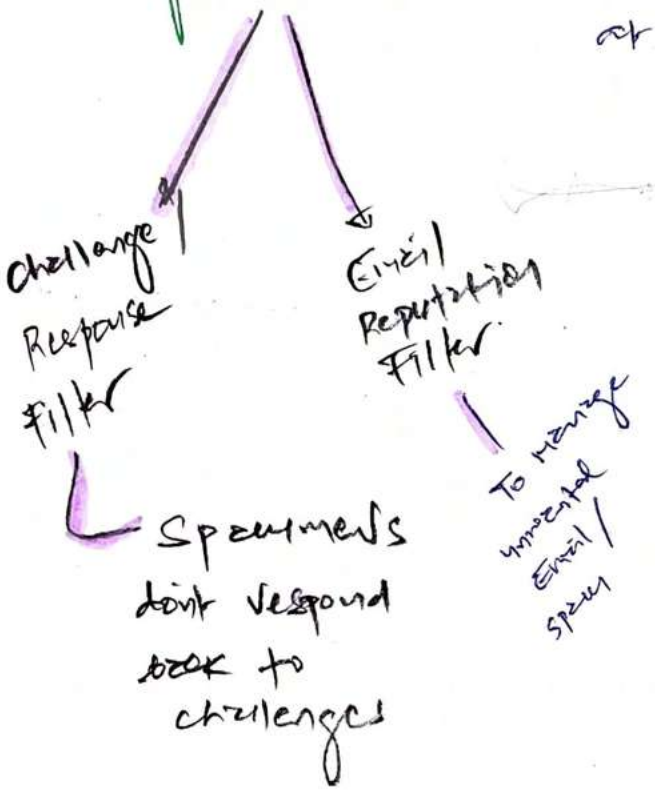
- Ensure valid email is sent through verification of domain identity.

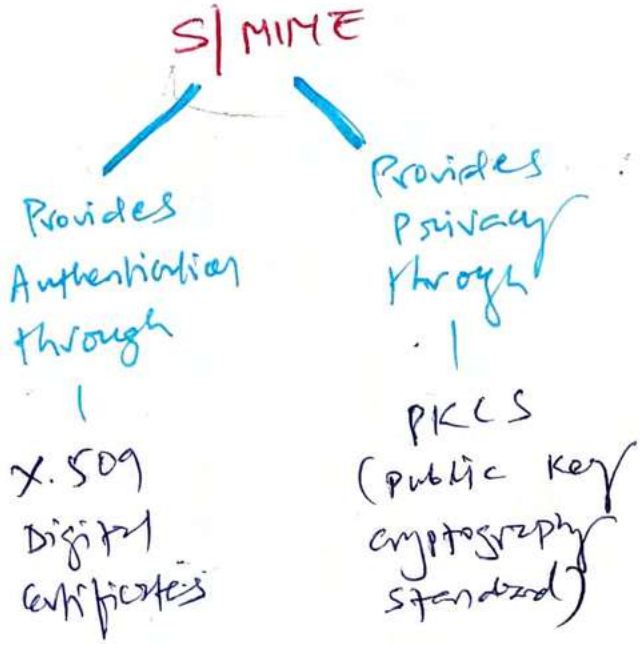
Email security at Glance

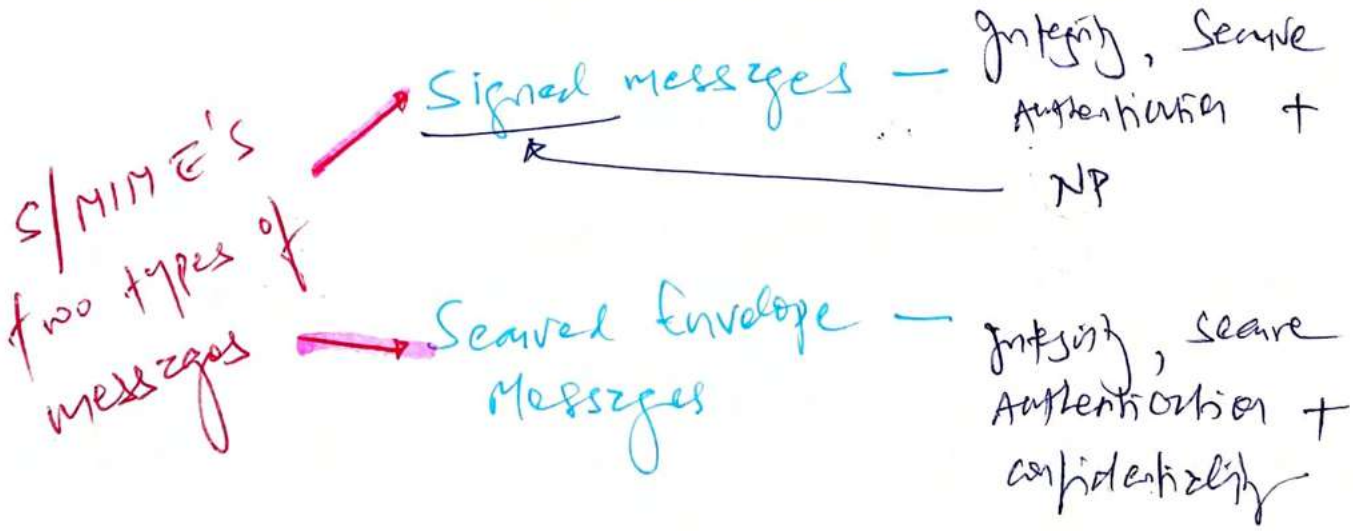
Digital Signatures → Eliminate impersonation

Encryption of messages → Reduces Eavesdropping.

Use of Email Filters → Keeps spamming & mail-bombing at minimum.







Telephony then →

- Plain Old Telephone Service (POTS)
  or
- Public Switched Telephone Network (PSTN)

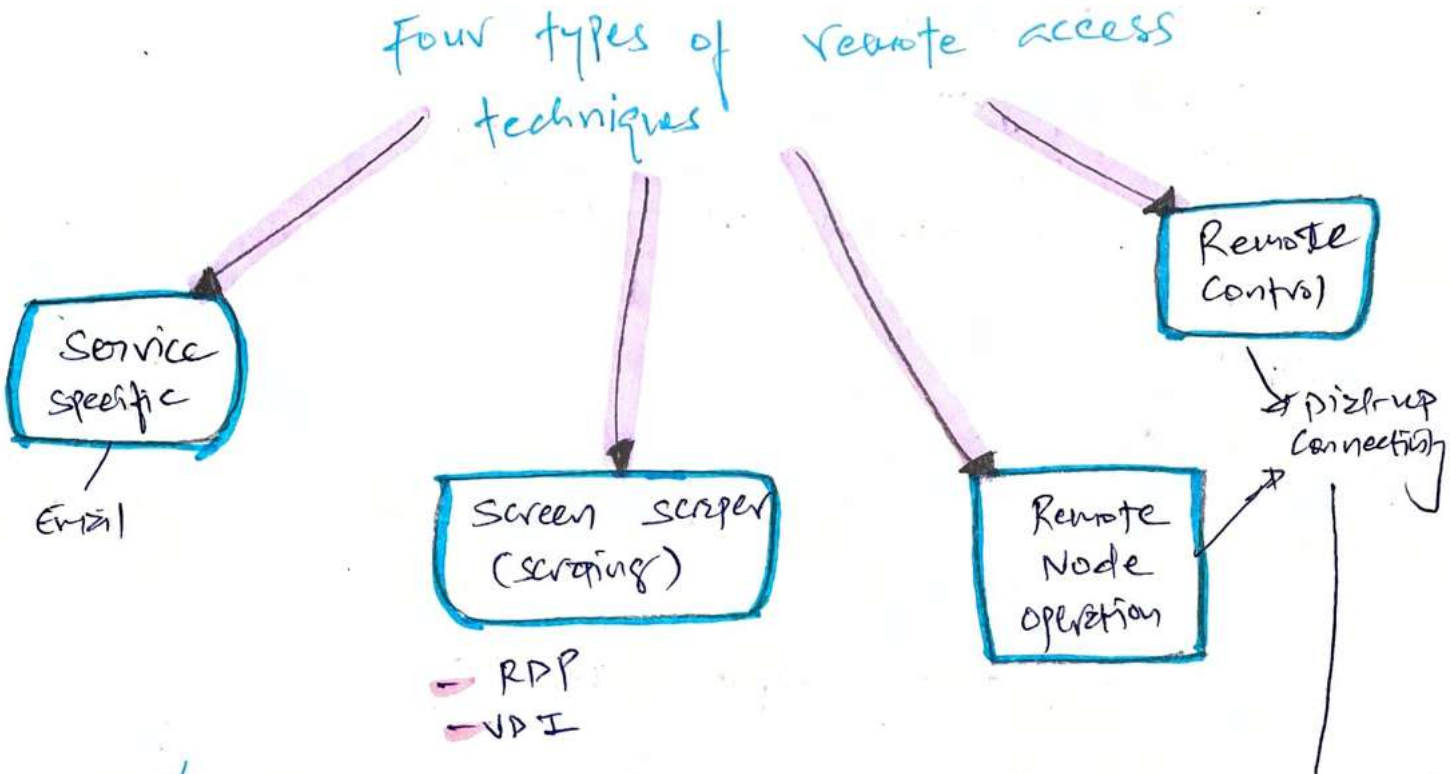
Combined with modems

Telephony Now →

- Private Branch Exchange (PBX)
  - VoIP
  - VPN

For telephone comms

✱ Remote Access Security Management



Plan / Address Remote Access Security Issues

Dial-up Protocols

Provides link governance for dial-up & VPN links

LCP uses encapsulation when two devices wants to connect

NCP make sure PPP can integrate with other protocol

LCP

NCP

PPP

Not an authentication protocol. It's dial-up

older technology

SLIP

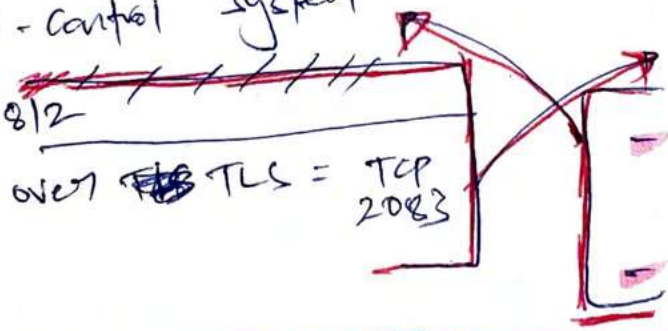
- Point-to-Point protocol
- Transmits TCP/IP packets over non-LAN connections such as: ISDN, VPN, Frame Relay
- choice for dial-up Internet connections
- Protected with CHAP & PAP
- PPP works on layer 2

- Serial line Interface protocol
- Support TCP/IP comms over asynchronous serial connections such as Serial cables, modem dial-up.
- Support only IP, require static IP, offers no error detection/correction, does not support compression.

Centralized Remote Authentication Service

TACACS+

- Terminal Access-controller Access-control System
- UDP 1812
- RADIUS over ~~TLS~~ TLS = TCP 2083



RADIUS

- Remote Authentication Dial-in User Service
- TACACS, XTACACS & TACACS+
- TACACS+ port TCP 49
- 2FA

RADIUS & TACACS provides seperation of authentication & authorization for remote clients, so if it's compromised, only remote connectivity is affected.

☆ Multi-homed Firewalls ☆

(Dual-homed)

has at least two interfaces to filter traffic

Note — All multi-homed firewalls has IP forwarding which automatically send traffic to another interface

should be disabled

Bastion Host / sacrificing host

- Exposed to internet that has been hardened by removing unnecessary services/ programs/ protocols & ports

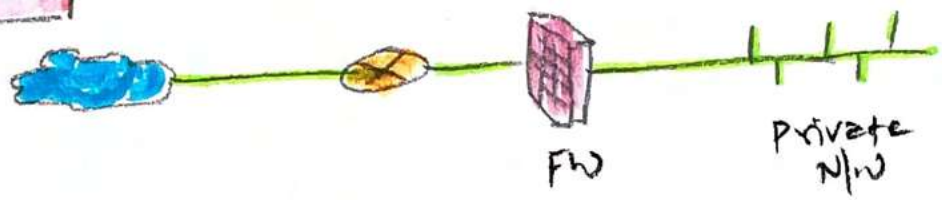
Screened Host / proxy host

- firewall protected system typically positioned just inside private network.
- All inbound traffic routed to screened host, it act as a proxy for all trusted system, responsible for filtering traffic + protect the identity of internal client.

Note — All inbound traffic is directed to bastion host, and only authorised traffic can pass through router/ firewall to private n/w.

☆ Firewall Deployment Architectures ☆

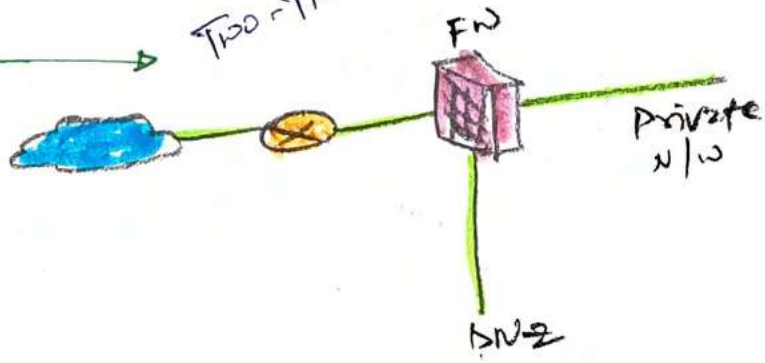
Single Tier



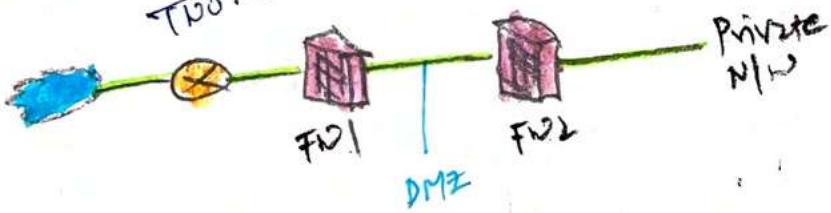
- minimal protection
- Useful against several Attacks

Two-Tier

Design 1 → Two-Tier I



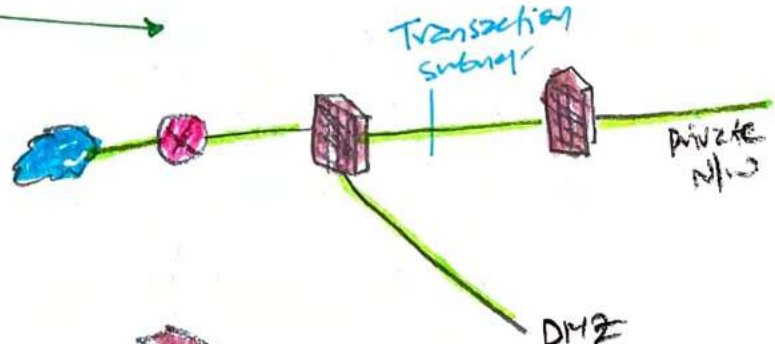
Design 2 → Two-Tier II



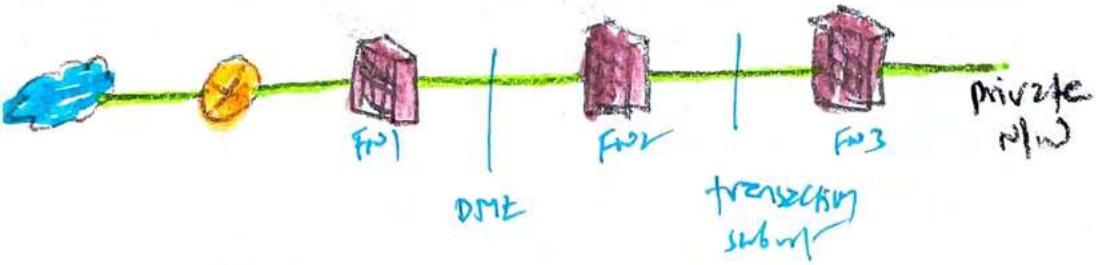
- moderate level of routing & filtering complexity.
- DMZ is used to host information for external users such as web/file servers

Three-Tier

Design 1 (Tier II)



Design 2 (Tier I)



- Most Secure

याद रखो

Cabling Types

10 Base 2 — Distance 185 meter
speed ↳ 10 mbps

10 Base 5 — 500 meter
speed ↳ 10

10 Base T — 100
(UTP)
speed ↳ 10 100

STP — ~~100~~
↳ 155

100 Base T / 100 Base Tx — 100
↳ 100

1000 Base T — 100
↳ 1 Gbps

Fiber Optic — 2+ km
↳ 2+ Gbps

Utp categories

	Throughput
Cat 1	voice only
Cat 2	4 mbps
Cat 3	10 mbps
Cat 4	16 mbps
Cat 5	100 mbps
Cat 6	1000 mbps
Cat 7	10 Gbps

Teardrop — Use of fragment TCP packets to target flaw in TCP / tcp stack fills resulting DoS.

Attacks

Christmas — Set all possible TCP flags on packet

↳ Challenge for Endpoint security = sheer volume of data

↳ Data leakage or anything that bypass security like data loss prevention = covert channel

↳ PPP has replaced SLIP. PPP is the answer for legacy service.

↳ Firewalls can't filter Non-IP protocols (IPX / SPX, NetBEUI, AppleTalk)

12. SECURE COMMUNICATIONS AND NETWORK ACCESS CONTD.

✡ VPN

DAMN GOOD INTERVIEW QUESTION - What is tunnel in Internet?

Encapsulation = creates logical illusion of communication tunnel

SNAIL MAIL

letter = primary content protocol packet

Envelope = tunneling protocol

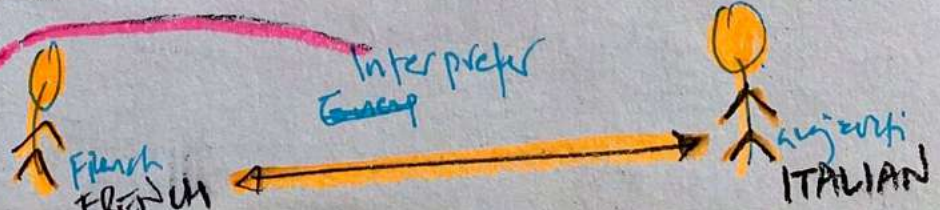
this creates security issue

- Hard to monitor content of the traffic

Tunneling problems

- Use larger packets = bandwidth saturation
- Not designed for broadcast as tunneling use point-to-point comms

VPN TRIVIA — Most VPN use encryption to protect encapsulated traffic, but encryption is not necessary for connection to considered a VPN.



* Common VPN Protocols

PPTP → Encapsulation protocol

offers Authentication

- operates @ Data Link layer 2 @ OSI
- Doesn't support RADIUS & TACACS+
- Supported protocols: CHAP, PAP, EAP, SPAP, MS-CHAP
- Initial PPTP session = Not Encrypted
- PPTP used on VPN, replaced by L2TP that uses IPSec for Encryption

* Most widely used PPTP adopted Microsoft P-2-P Encryption that supports data Encryption.

L2F

- Mutual authentication tunneling mechanism
- No Encryption
- Replaced by L2TP
- layer 2 @ OSI

L2TP

- Provides point-to-point tunneling
- No in-built encryption, relies on IPSec for Encryption
- Supports RADIUS & TACACS+

IPSec

- layer 3 @ OSI
- only for IP networks
- Provides secure authentication + encrypted data transmission

AH & ESP requires 2 security Associations each = total 4 SA

Authentication → AH
Encryption → ESP

- Auth, NP, I
- Encryption + limited Auth

Transport mode: only IP packet data is encrypted, not header

Tunnel mode: Entire IP packet is encrypted

ESP provides Encryption & limited authentication

VPN characteristic Table P544

VPN PROTOCOL	Native Authentication Protection	Native Data Encryption	Protocols Supported	Dial-up Links Supported	Number of Simultaneous Connections
PPTP	yes	No	PPP	yes	Single Point-to-point
L2F	yes	NO	PPP/ SLIP	yes	"
L2TP	yes	No (can use IPsec)	PPP	yes	"
IPSec	yes	yes	IP only	No	Multiple

Vlan Notes

Vlan works like subnets. But, they are not actual subnets.

Vlan used for → Traffic mgmt

Vlan Mgmt → Control Vlan traffic for Security or performance

- Vlan restricts broadcast traffic
- Reduce network's vulnerability to sniffers with isolation / segmentation
  - Isolated private vlans
- Layer 3 switch prevents broadcast storms
  - Flood of unwanted Ethernet broadcast network traffic.
- Define no routing b/w vlan or deny filter b/w certain vlans.

✱ Virtualization

Security

- Easy Backup (A)
- Safer testing

VM Escaping

- when software within guest OS is breached

To minimize Risk

1. Have physical isolation (servers) for sensitive Data
2. Monitor
3. Patch hypervisor software up to date

✱ Virtual Software

running windows Application on Linux host or USB

Virtual Desktop

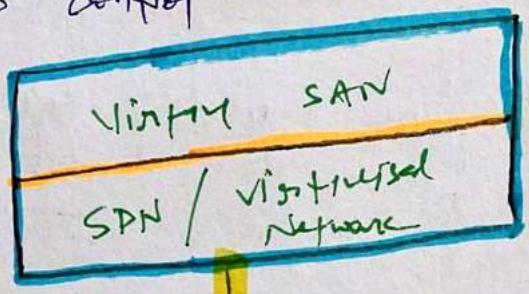
refers to

- Remote Access Tool
- Extension to virtual App
- Expanded Desktop

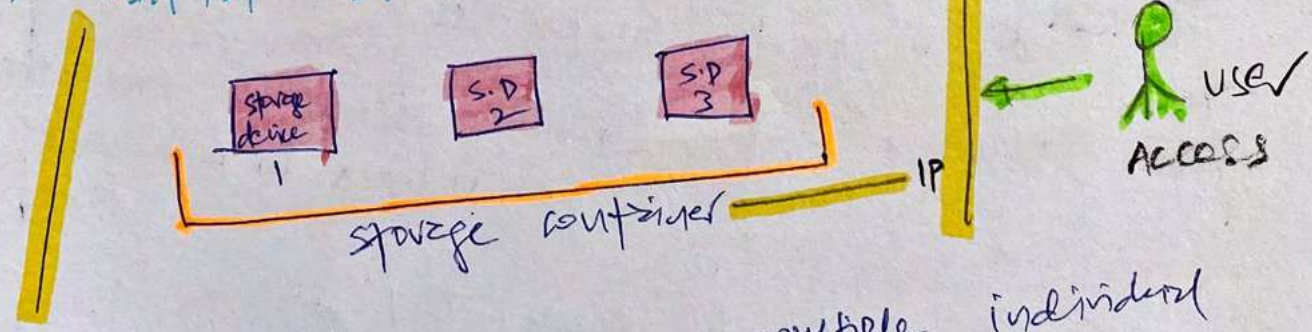
* Virtual Networking

Software Defined Networking (SDN)

- Vendor neutral + independence
- From IP to programming + routing
- SDN seperates infrastructure / hardware layer from control layer
- Allows data transmission paths, communication decision trees & flow control



* Virtual SAN



A technology that combines multiple individual storage devices into single consolidated - network - ~~accessible~~ accessible storage container.

→ Virtual SAN is software-defined shared storage system, is a virtual overlay of SAN, on top of virtualized network or SDN.

✱ Network Address Translation (NAT) --- layer 3 @ OSI

NAT : Internal IP → External IP

PAT : Internal IP → External IP + port number

multiplexing of or NAT overloading

NAT

Private IP Range

10.0.0.0 – 10.255.255.255 — A

172.16.0.0 – 172.31.255.255 — B

192.168.0.0 – 192.168.255.255 — C

You can never route a traffic on private IP Address (RFC 1918). Routers in Internet will drop data packets containing source or destination for RFC 1918 ranges.

NAT
- Static
- Dynamic

→ P.t.o (more detail)

NAT-Traversal (RFC 3947) - designed to support IPsec VPN through UDP encapsulation of IKE.

Automatic Private IP Addressing (APIPA)

169.254.0.1
to 169.254.255.255

Assign IP if DHCP fails

APIPA = problem

- Power failure on DHCP
- Bad cable
- Malicious attack on DHCP server

Note – APIPA & loopback (127.x.x.x) are not private IPs.

Stateful NAT → Maintains information about the communication sessions b/w internal clients & external systems.

NAT & IPSec – NAT is not directly compatible with IPSec as NAT modifies packet header, And IPSec too rely on encrypting packet header for security. Thus, we have to use NAT-Traversal.

Read Table 12.2 (p555)

✱ Switching Technologies.

p.t.o for list

Circuit switching

- Telephone network
- Permanent physical connections
- Fixed transmission times, uniform level of quality, little to no loss of comm interruptions.
- once path is disconnected, diffrent path may assemble after reconnection.
- offers Exclusive use of communication path → Nope.

Packet-Switching

- Connectionless
- sensitive to data loss
- Message broken into smaller segments.
  - Each segment has its own header, src, dst IP that routes from hop to hop.
- Unlike circuit s/w, if path is broken, it's easy to find alternate path but have to encrypt packet to prevent from data disclosure.

Virtual Circuits

← Multiple path exists b/w point A & B

- logical pathway or circuit created over packet-switch network b/w two endpoints.

2 types

predefined → PVC = Walkie Talkie

Have to create → SVC = DIAL-UP

Permanent VC (PVC)

- Two-way radio or walkie-Talkie
- Predefined VC, always avilable, Press button & start talking.

Switched VC (SVC)

- Shortwave radio = requires tuning
- Like dial-up connection, VC to be created, best path chose from multiple routes, disassembled after use

* WAN Technologies

2 types of WAN links:

Dedicated line (leased line / point-to-point link)

- Dedicated line is always open & waiting for traffic to be transmitted over it. (Eg. customer LAN to WAN)
- T_1
- T_3
- E_1
- E_3

Nondedicated line

- Requires connections to be established before transmission can occur.
- DSL, ISDN & standard modems

For Exam

DSL - Digital subscriber line

- A technology that exploits the upgraded telephone network to grant customer speeds from 144 Kbps to 20Mbps & more

DSL formats:

- ADSL
- xDSL
- CDSL
- HDSL
- SDSL
- VDSL
- IDSL
- RADSL

- Max. DSL line distance = 5000 meters

* ISDN
(Integrated Services Digital Network)

- ISDN is fully digital telephone network that supports both voice and high speed data communications.

ISDN Formats

(BRI)
Basic Rate Interface

- 144 Kbps as total throughput
- offers customer connection with
  - two B channel & one D channel
    - 64 Kbps throughput
    - used for Data trans.
    - used for call establishment, mgmt & tear down
    - Bandwidth 16 Kbps

(PRI)
Primary Rate Interface

- 192 Kbps to 1.54 Mbps as bandwidth, not throughput
- multiple 64-Kbps B channels (2 to 23)
- single D chan 64 Kbps

WAN Notes

↳ CSU/DSU (channel service unit / Data service unit) device converts LAN signals to WAN carrier npo & v.v

↳ CSU/DSU contains DTE/DCE (Data terminal equipment/ Data circuit-terminating Equipment), that provide actual connection point for LAN router (DTE), WAN carrier npo switch (DCE)

* WAN Technologies for connection

X.25

- older packet-switching technology
- Uses PVC for P-2-P connection
- lower throughput + performance

SMDS

- Switched multimegabit Data Service
- Connectionless packet-switching
- Connect MAN, remote LAN
- Fragment data into small fragmentable cells

FRAME RELAY

- layer 2 @ OSI, Packet-switching
- Use of multiple PVCs, connection oriented
- CIR (committed Info. Rate)
- Requires use of DTE / DCE
  ∴ LAN ∴ WAN

ATM

- Asynchronous Transfer mode
- Connection-oriented
- Cell-switching WAN Technology
- Fragments comms into fixed length 53-byte cells
- Use PVC &/or SVC
- offers high throughput

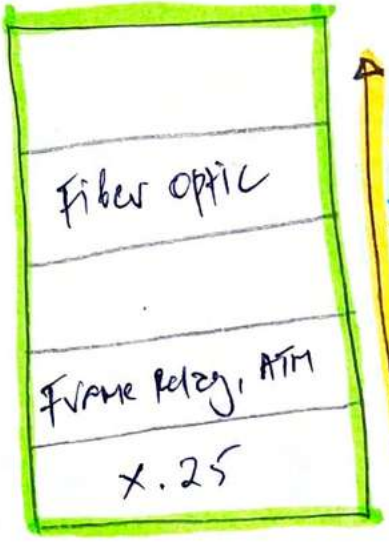
SDH

- Fibre
- ITU
- Synchronous Digital Hierarchy

Both use time-division multiplexing (TDM) with minimum control & mgmt overhead.

SONET

- Fibre
- American — (ANSI)
- Synchronous optical Network
- * SONET + SDH use time division multi. (TDM) to high-speed duplex communications.
- SDH+SONET support mesh & ring topologies. often implemented as backbone for Telcos
- SDH+SONET interception point is ADM (Add-Drop multiplexers) - allows addition and removal of low rate bit stream connections.



* Specialized Protocols

Synchronous Data Link control

SDLC

upgrad version

High-Level LC

HDLC

- Use of permanent physical connection of dedicated leased lines to provide connection to mainframe sch as IBM system

- Refined version of SDLC for serial synchronous connections

- supports full duplex, P-2-P, P-2-M

- SDLC uses polling @ layer 2 OSI, and is bit-oriented synchronous protocol

= + Flow control, Error correction & detection

HSSI

High-speed LC

- layer 1 @ OSI
- HSSI is DTE/DCE interface standard that defines how multiplexers and routers connect to high-speed network such as ATM/ Frame Relay.

* Dial-Up Encapsulation Protocols

PPP - Encapsulation protocol designed to support transmission of IP traffic over → dial-up
→ point-to-point links

Replaced Slip

- All dial-up & P-2-P connections are Serials in nature.

✡ PREVENT OR MITIGATE NETWORK ATTACKS

p.t.o

p.t.o for prevention

DoS

- resource consumption attack

2 forms

- Attack exploiting vuls. in H/w & S/w
- Flood victim's pipeline with garbage

Result: computer unable to process legitimate requests.

DDoS

- DDoS Attack that use intermediary system as secondary victims using Zombie, bots, agents = DDoS

→ this entire thing/ deployment is called BOTNET

Replay

- Attack using captured traffic via eavesdropping
- Reestablish comm session against the system
- Prevent using onetime Auth. mechanism and sequence session identification

Eavesdropping

- Dangerous for data in transit than data at rest
- Passive attack that requires physical access to IT infra
- wireshark, sniffer, ZAP (zed Attack proxy)

Impersonation / Masquerading

when username & password is captured

- Pretending to be someone (@hacktivist) ← :(
- Different from Spoofing: false identity without proof
- Use onetime pad / token Auth. using kerberos

Modification Attacks

- this attack bypass this
- Captured packets are altered and then played against the system
- Prevention: Digital signature verification & packet checksum verification

DNS poisioning & DNS spoofing are called RESOLUTION ATTACKS.

ARP Spoofing

- Provides false MAC address for requested IP Address, then system redirect traffic to alternate destinations.
- ARP Attacks are often elements in MITM Attacks.
- Prevention:
  - Use static ARP mapping for critical systems
  - Monitor ARP caches for MAC-to-IP Address mapping
  - Use IDS to detect anomalies in traffic and change in ARP traffic.

DNS poisioning

- When Attacker alters domain name to IP Address mapping to redirect traffic to rogue system

DNS Spoofing

- Exploitation of Race conditions
- When Attacker sends false replies to requesting system, beating the real reply from valid DNS server

DNS Hijacking

- Sending false reply to caching DNS server for nonexistent subdomains, attacker can hijack entire domain registrations details.

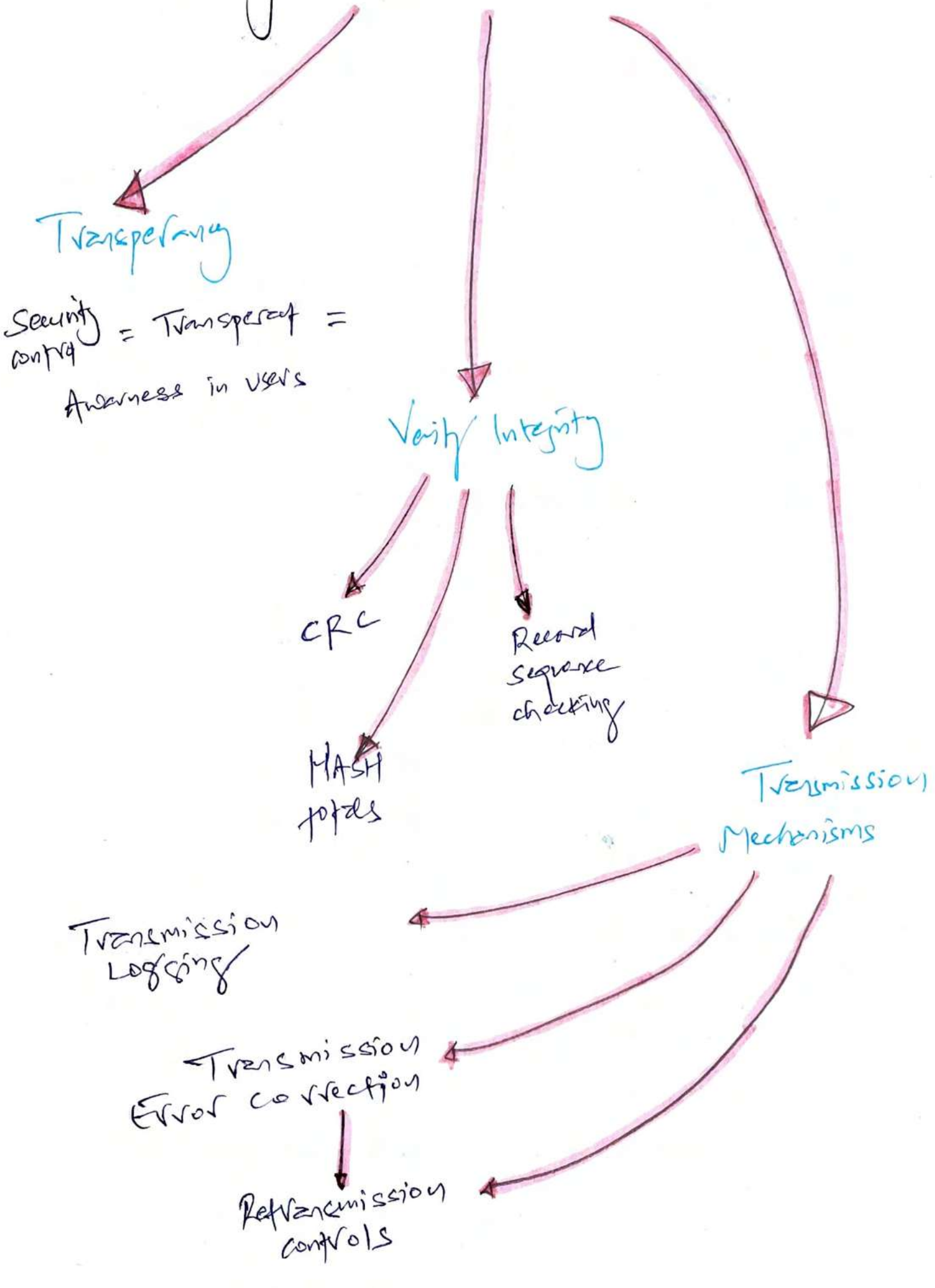
Note - only solution for DNS hijacking is to upgrade DNS to DNSSEC

Hyperlink spoofing

This attack

- Can take the form of DNS Spoofing or simply an alteration of hyperlink URL in HTML code of domain Send to client
- Who see the URL anyway - this attack is usually ~~successful~~ successful — click, click, click

Security Control characteristics



Network Attack Preventions

DoS / DDoS

- Add FW / Router / IDS that detect DOS Traffic
- Disable & block broadcast features, ICMP / Echo reply & spoofed packets
- Upto date system patch
- Consider commercial DoS protection or Response like Cloudfare / Prolexic

Eavesdropping

- Onetime Authentication methods (token devices)
- Use of Encryption (SSH, IPsec)
- Physical control to prevent access from unauthorised personals
- Software installation policy (not everyone should be able to install Wireshark)
- IAM / Least privilege on System access

Impersonation / Masquerading

- Use of onetime pad, authentication token, Kerberos, encryption

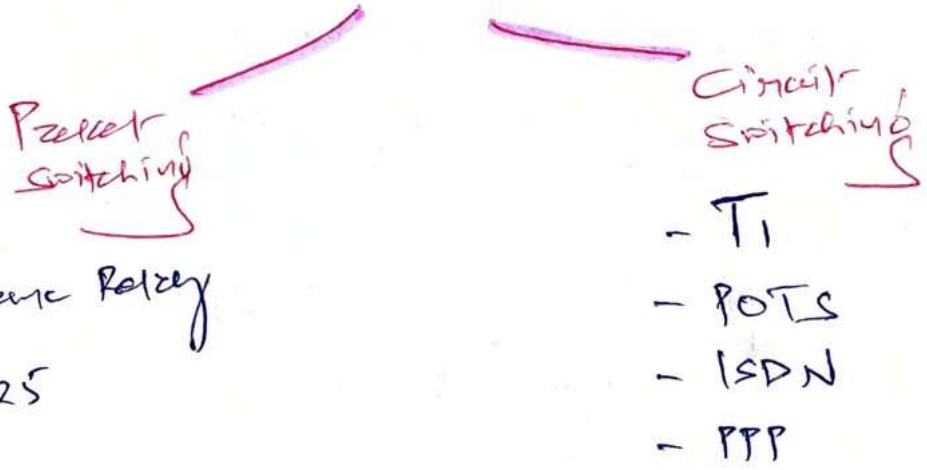
PBX Notes

DISA (Direct Inward System Access)

↳ Uses access codes assigned to users to add a control layer for external access & control of the PBX..

Compromise of access codes = Attackers can make calls through PBX & even control.

- ATM Cell — WAN Technologies



13. MANAGING IDENTITY & AUTHENTICATION

CORE - Management, administration & implementation aspects of GRANTING or RESTRICTING access to ASSETS.

PERSPECTIVE

Types of Access controls
- Preventive
- Detective
- Corrective

implemented As
- Administrative
- Logical (Technical)
- Physical

Four Primary Access control Elements
- Identification
- Authentication
- Authorization
- Accounting

IAM Implementation
- SSO
- LDAP
- Kerberos
- Federation + SSO
- scripted Access

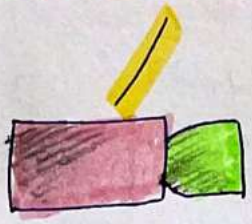
Authentication Factors
Type - I, II, III

AAA Protocols
- RADIUS
- TACACS
- Diameter

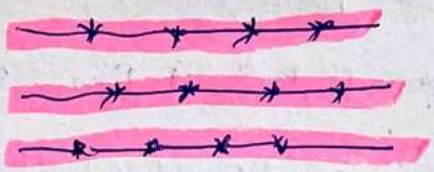
IAM Lifecycle
- Provisioning
- Account Review
- Account Revocation

* Types of Access control

Preventive Access Controls



CCTV



Fence

IPS + Firewalls

Antivirus software

Security policies

Security awareness & Training

Detective Access controls

motion detectors

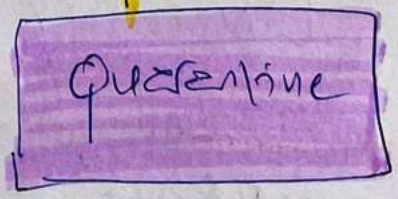
Security Guard

Job Rotation + Mandatory vacation

IDS + Honeypots

Corrective Access controls

Virus



modifies the environment to return system to normal after unauthorized activity or security incident such as

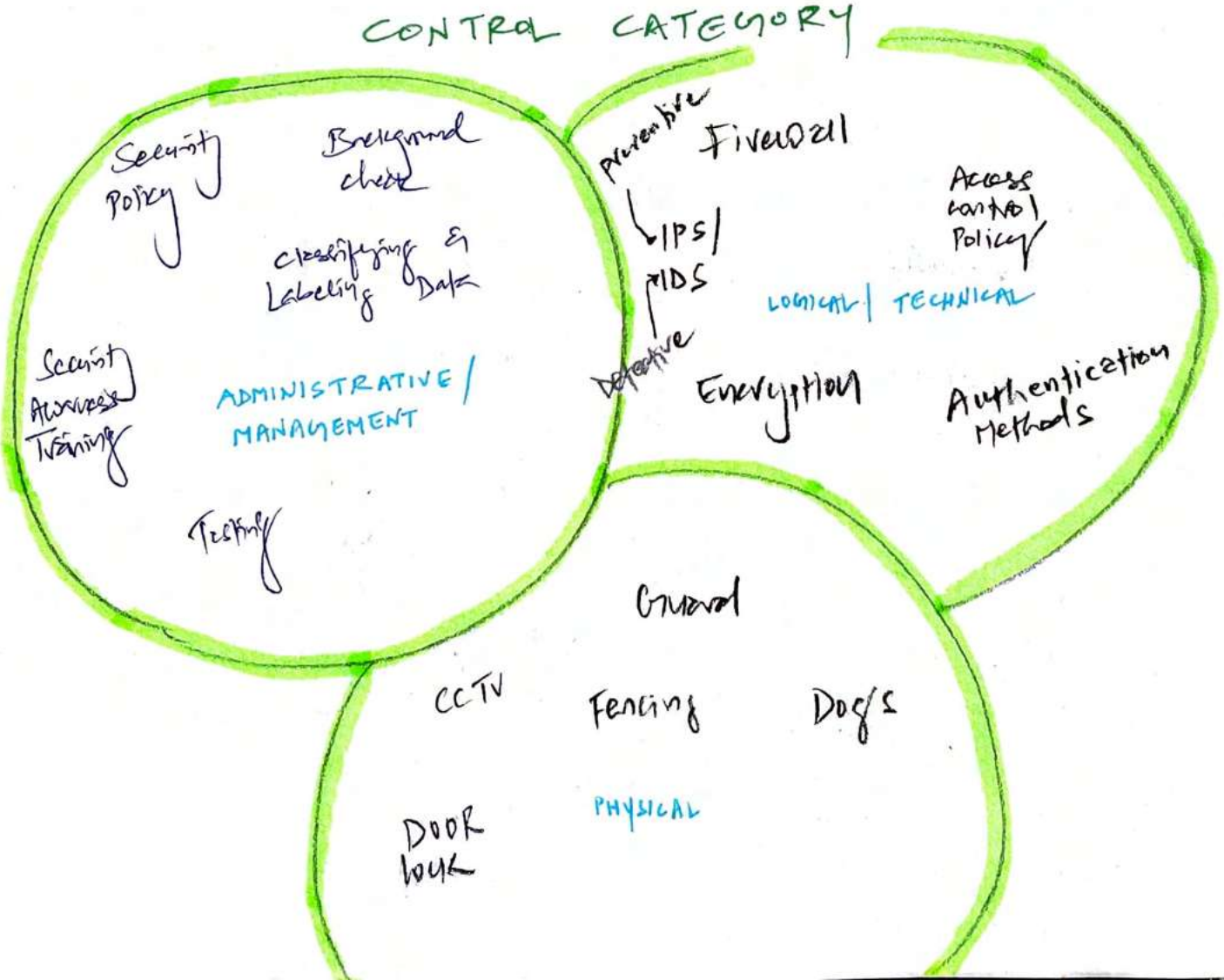
* other controls

Deterrent → Discourage → signboard / warnings

Recovery → It's different from corrective control as this is an about- Repair and Restore
→ backup & restore

Directive → Enforce security policy (compliance) | DETOUR SIGN

Compensating → Alternate



Effective identification + Authentication

+ Auditing

⇓

ACCOUNTABILITY

No Authorization

Identification + Authentication → Authorization → Accounting

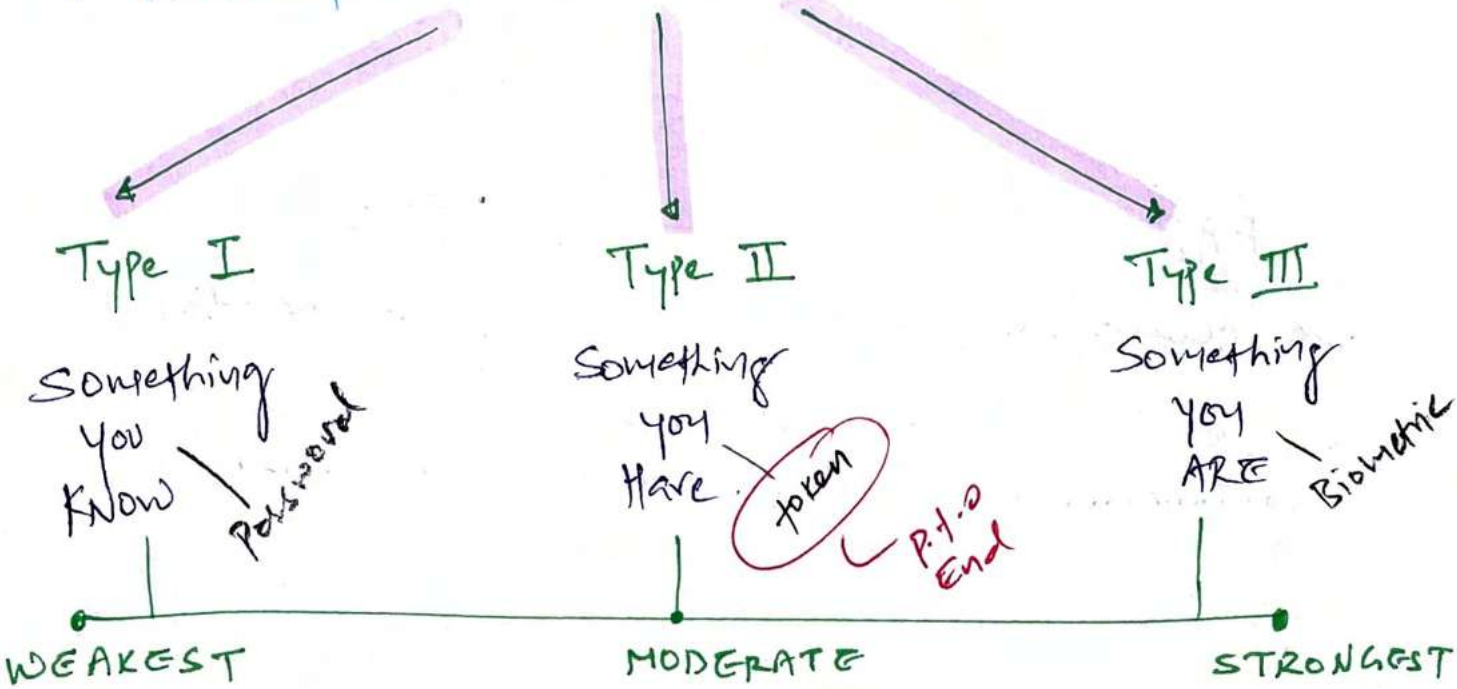
Logging user actions based on their proven identities provides

Logging + Monitoring + Auditing

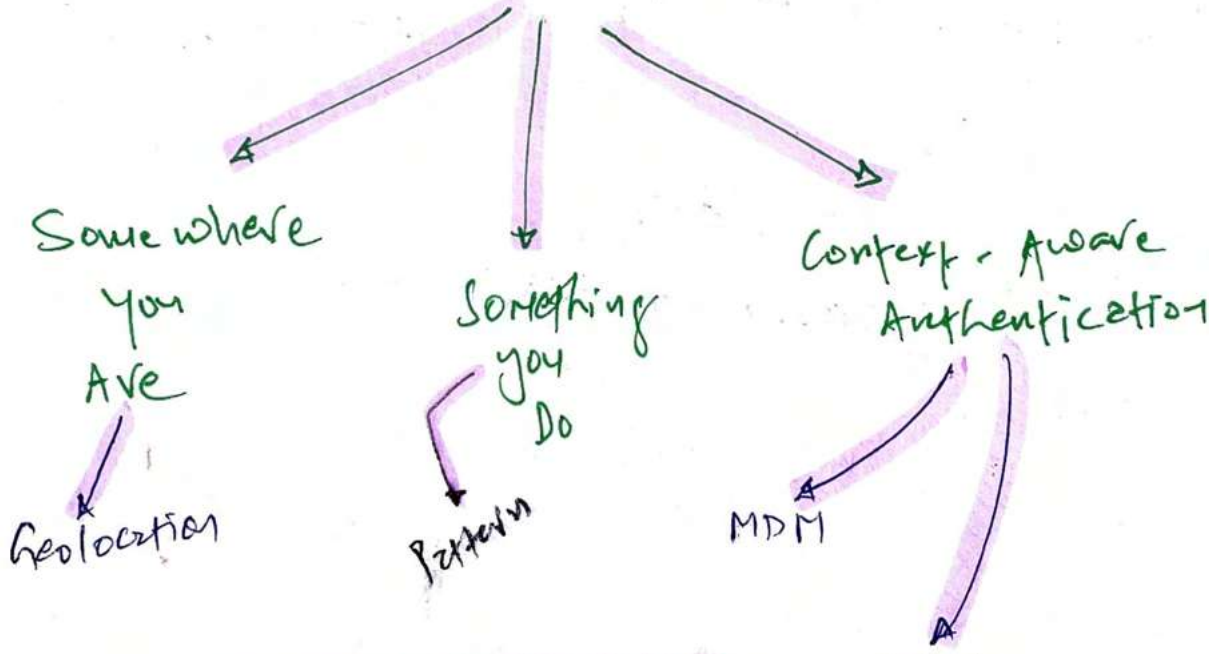
⇓

ACCOUNTABILITY

* Authentication Factors



* other factors



Two-step Authentication

HOTP
Hash-based one time password - value remains till used
↳ Network Code

TOTP
Time OTP - code expires such as 30-seconds

NOTE - what if OTP displayed on mobile as pop-up notification. How is that secure.
Check NIST 800-63B

Biometrics

Type 2 Error

FAR

(False Acceptance Rate)

- Invalid subject is authenticated
- False positive
  - Wrong guy is positive

or false positive is when invalid subject is authenticated

Type I Error

FRR

(False Rejection Rate)

- Valid subject is not authenticated
- False Negative
  - Right guy is negative

or false negative is when valid subject is not authenticated

CER

(Crossover Error Rate)

- To determine the quality of Biometric system

~~False~~ positive is better than false negative.

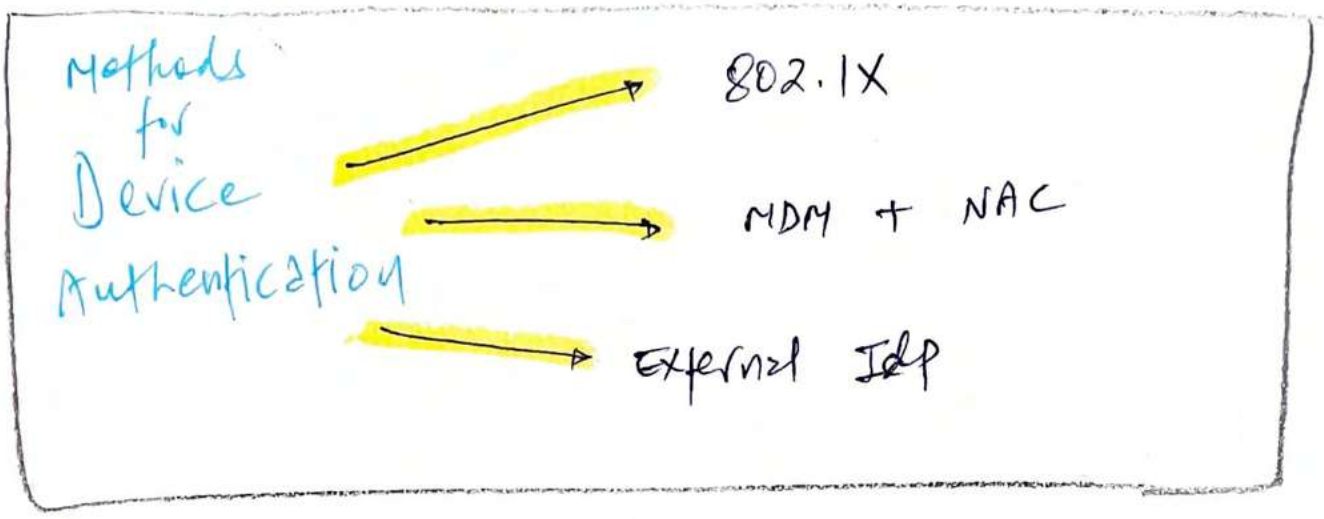
Biometric Device Sensitivity

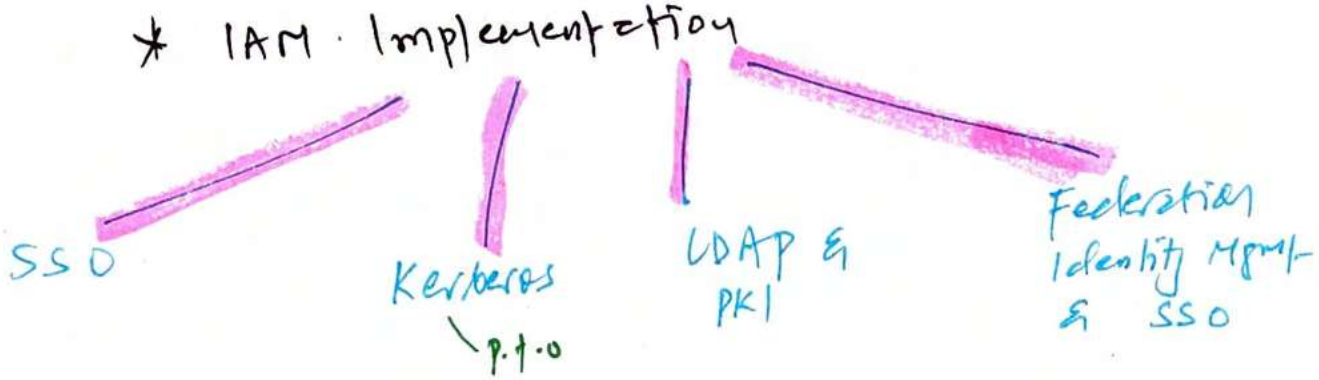
High
- FRR increases
- More false negatives

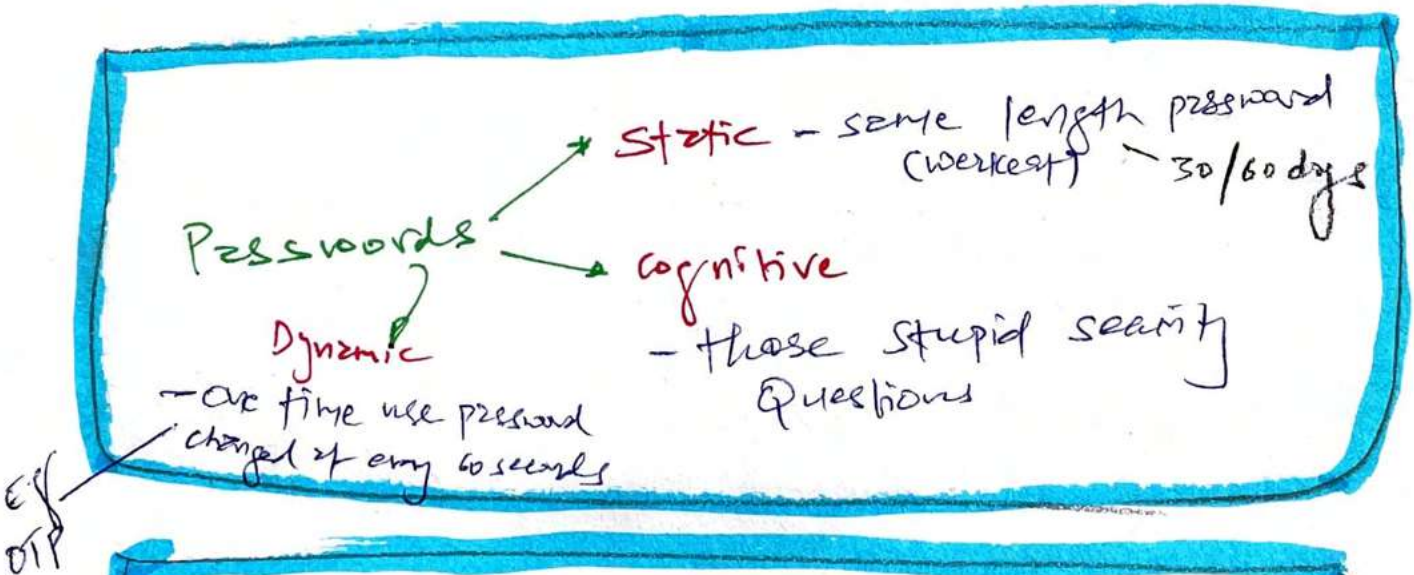
low
- FAR increases
- More False positives

↑ FRR → Prim for support

↑ FAR → Not good for security







Password Storage

Passwords are never stored in plaintext. Instead, system creates hash for password using hashing algorithm like SHA-3. For same password, it creates same hash number. when ~~we~~ User authenticates, System hashes the supplied password & matches with stored password hash, if it's same, system authenticates user.

Provides "C" + "I"

KERBEROS

→ Primary purpose = Authentication

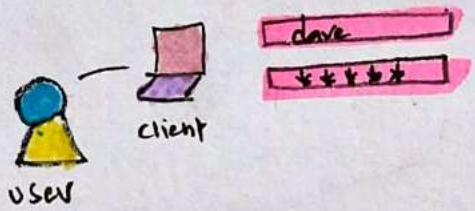
— deserves a video

↳ For SSO

P.T.O End for diagram

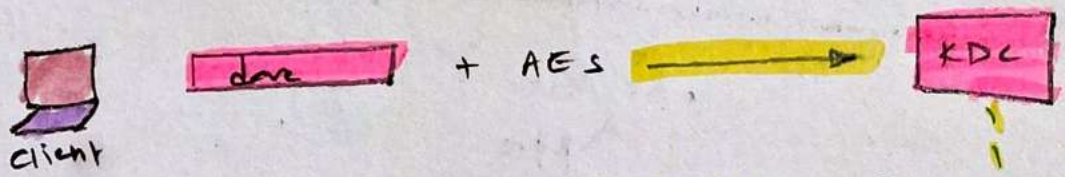
kerberos logon process

1



User types username & password into the client

2

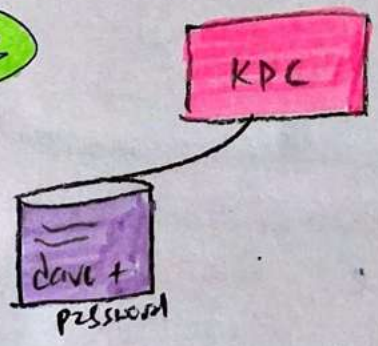


client encrypts the username with AES & send to KDC

All clients & servers are maintained in KDC

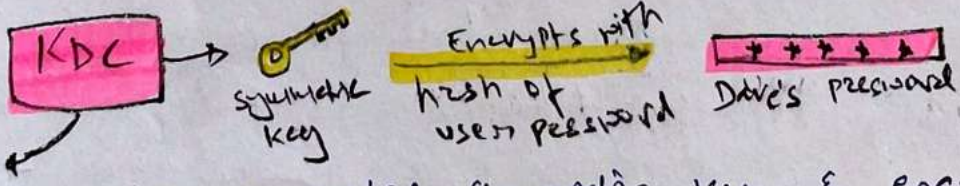
Key distribution centre - trusted 3rd party that provides authentication service using symmetric cryptography

3



KDC verifies username against database of known credentials

4



TGT

KDC generates symmetric key & encrypts with user password. KDC also generates time-stamped TGT (proof that subject is authenticated in KDC)

5. KDC transmits encrypted symmetric key & TGT to client.

6. client installs TGT for use until expires.

client decrypts symmetric key with user's password.

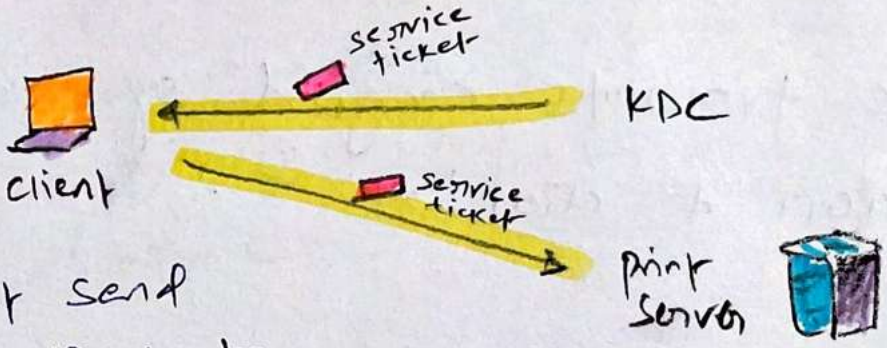
Note - Security is user password is never transmitted - the symmetric key will ~~encrypt &~~ decrypt if user know ~~the password~~

when client want to access object

1. client sends TGT to KDC with request to access resource (print)
2. KDC verifies TGT is valid & checks client has sufficient privilege to print the document.
3. 

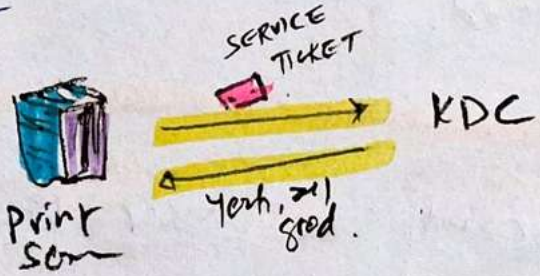
KDC generates service ticket & send to client.

4



client send service ticket to print server

5 Server verifies the validity of ticket with KDC



6 Kerberos activity is completed when identity & authorization is verified.

7 Session opens b/w client & server for a print job.

Note - Kerberos take care of CIA but need time-synchronised within servers & each other.

Kerberos problem
- KDC = single point of failure
- KDC down = No subject Authentication
- Require time synchronization

AAA Protocols

RADIUS ← not for SSO

- Remote Authentication Dial-in User Service
- Uses UDP and encrypts only the exchange of passwords
- Doesn't encrypt the entire session

(improvements)

Diameter

- TCP port 3868
- Supports IPSec & TLS

TACACS

- Terminal Access controller Access-control system
- TACACS+
  - ↳ Encrypts all of the authentication information
  - ~~↳ UDP port 49~~
- TACACS+
  - ↳ TCP 49 (Reliability)

RADIUS → Centralizes authentication for remote connections

TACACS+ → Seperates Authentication, Authorization & Accounting into seperate processes

Diameter → supports traditional IP, mobile IP, VoIP

Federated Identity Management & SSO

End P.t.O

Revised concepts from All-in-one

A common language to communicate with different federation organizations.

SAML — Security Assertion Markup Language

- For SSO
- Exchange Authentication & Authorization (AA) information b/w federation organizations.

SPML — Service provisioning Markup language

- Exchanges user information for federated identity SSO purpose.
- Allows platform to generate & respond to provisioning requests.

XACML — Extensible Access control Markup Language.

- For s/w defined n/w Apps
- Implements policies in attribute-based access-control system + also uses RBAC.

OAuth 2.0 — Open Authorization

- Signup to canva using Twitter credentials.

P.t.O

OpenID — Decentralized Authentication

↳ User can login to multiple unrelated websites with one set of credentials maintained by 3rd party

OpenID Connect — Authentication layer using OAuth 2.0 framework

↳ Use of JSON (Javascript object Notation) + JWT (JSON web token)

OAuth + OpenID } — for web based Apps to share Authentication info. without sharing credentials.

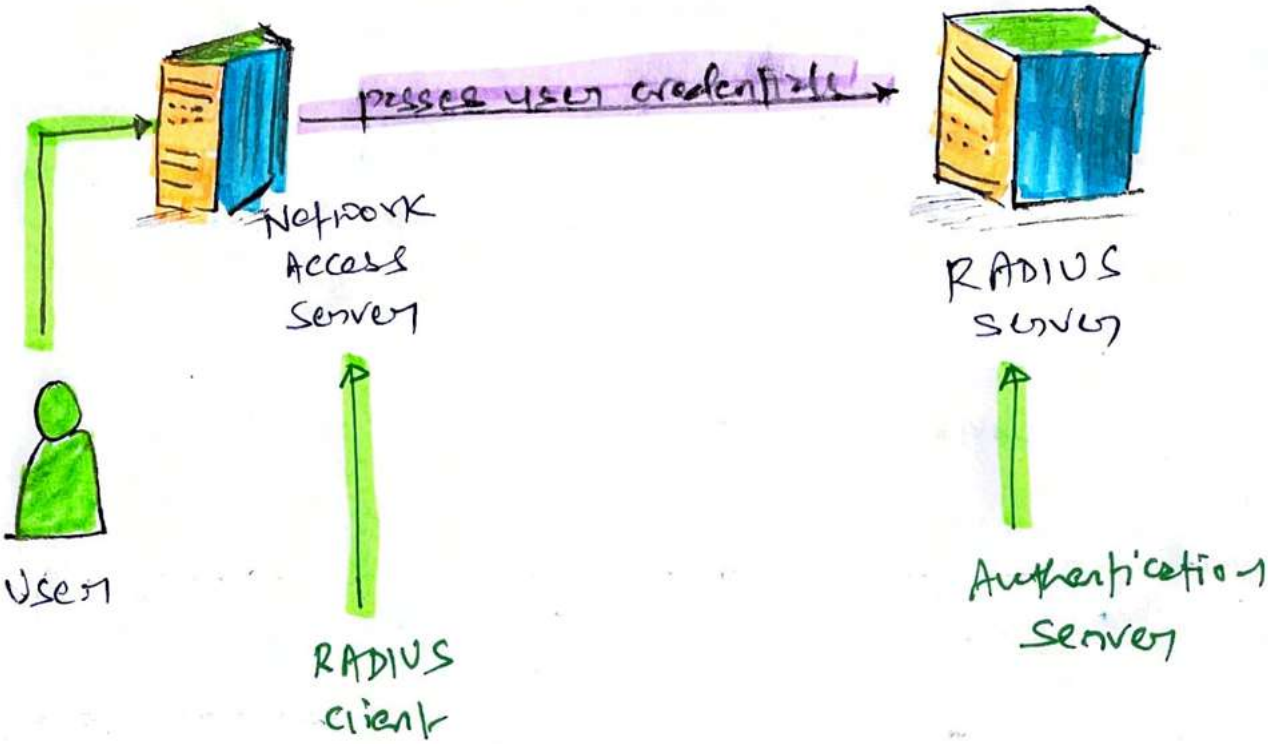
OAuth — Allows access to resources from another service

OpenID — Allows to use account from another service with user application

Kerberos + LDAP — In-house services

LDAP — P.T.O — End xx

RADIUS Architecture



Kerberos
ADFS
Central Authentication Service (CAS)

} ✓ SSO

RADIUS × SSO

Biometric Errors (p.t.o summary)

- Type I – Valid subject is not authorised
- Type II – Invalid subject is incorrectly authenticated as a valid user

Tokens

Synchronous Dynamic Password Tokens

time based passwords that Expires in 30/60 seconds.

Asynchronous Dynamic Password Tokens

- uses algorithm / counter where password / code is active until it used

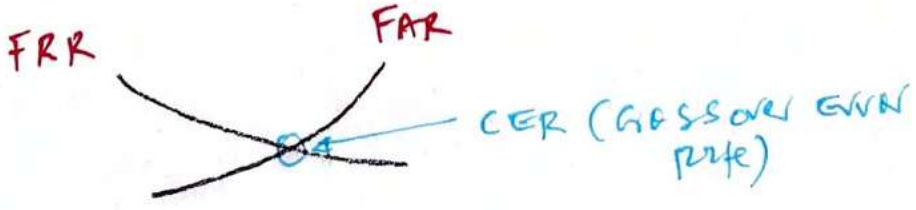
Biometic Ultimate summary

Type I — FRR — False Rejection Rate

- Valid subject not authenticated
- False negative
- High sensitivity = more FRR / false negatives

Type II — FAR — False Acceptance Rate

- Invalid subject authenticated
- False positive
- ~~High~~ Low sensitivity = more FAR / false positives



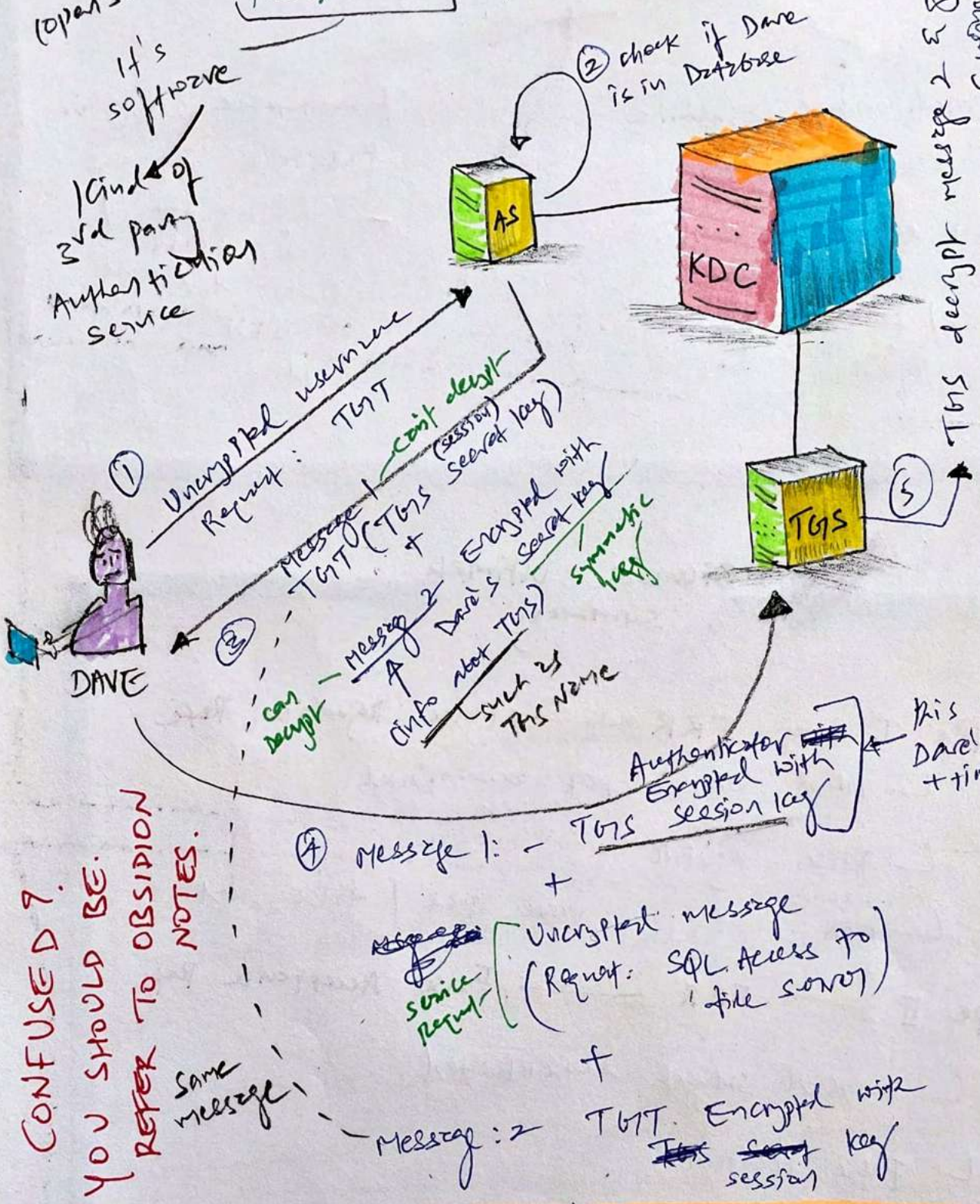
- low CER = Accurate Biometic System
- False Negative is better than False positive

Kerberos From Luke A.

(open source)

It's software

Kind of 3rd party Authentication service



CONFUSED?
YOU SHOULD BE.
REFER TO OBSIDION NOTES.

1. TGT is used to communicate TGS. TGS send service ticket to client to access the resource.
2. TGT has TGS session key. only TGS can decrypt TGT.
3. KDC (AS + KGS) generates session specific key that can be decrypt with user's password for short, AS+KGS & user, all three know session key

Perspective

KDC

- KDC vouches for individual's identities using tickets.

CA

- CA ~~validate~~ vouches for individual's identities using Digital certificates.

Attacks

- **Dictionary** — all possible common password words, with possible combinations
- **Brute-Force** — all possible key values
- **Rainbow table** — when attackers already has hash of the passwords

---

storage device → X

- User 1: read, write
- User 2: read
- User 3: read, write, delete

what type of Access control is used?

→ Resource-based Access control

Matches permission to resource like a storage volume. They are common in cloud-based infra.

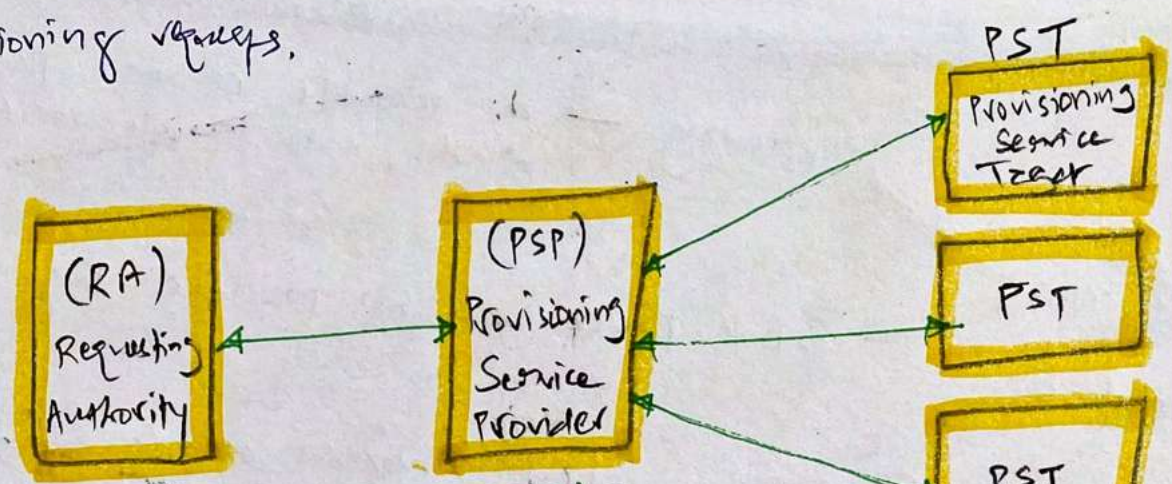
- ✗ RBAC
- ✗ MAC
- ✗ RUBAC

SPML - Service Provisioning Markup Language

Core purpose → SPML helps to ease of user account mngmt (a/c creation, modification, deletion) in complex environment

↓

Designed to allow platforms to generate and respond to provisioning requests.



Initiates a/c request for new employee

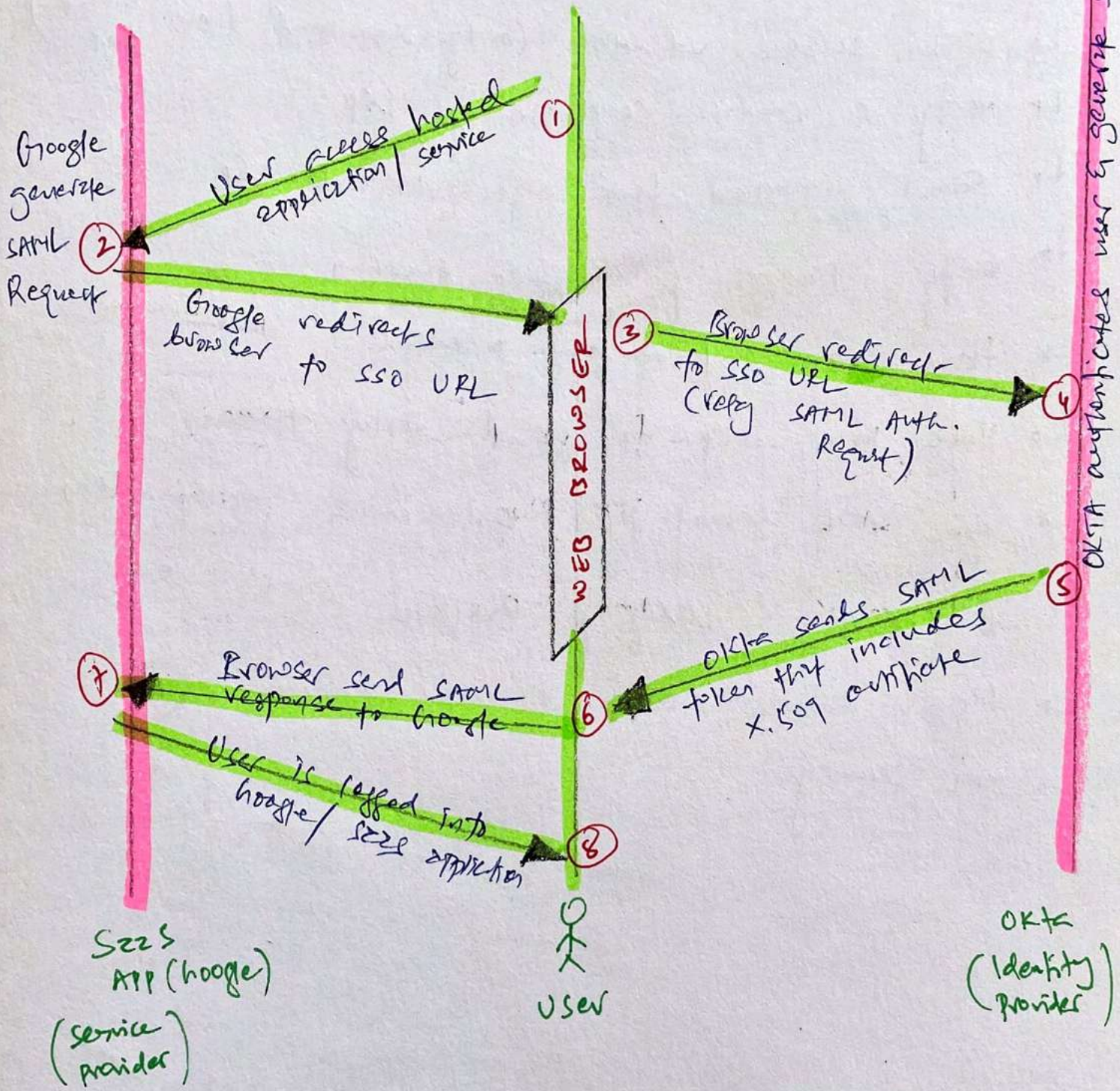
Revied request & compare with organization's accepted criteria

Setup necessary a/c & configurations for access rights

Note - SPML is designed for exchanging user information for federated identity SSO purpose.

SAML - Security Assertion Markup Language

(security concerns - P.T.O)



Note - SAML exchanges Authentication & Authorization information b/w federate identities

Note - SP & IDP already established trust using PKI (x.509) before SAML.

Note - Identity Provider is a single point of failure. think Backup Authentication.

* SAML Security Concerns / Precautions

- Use TLS to secure SAML token
- XML schema validation (only download from trusted IDP)
- Verify & validate certificate of IdP
- Secure connection from application to IdP (IPSec)
- Verify strength of encryption Algorithm
- Have strong AD/ ~~window password~~
- Have proper NTP to prevent replay attacks.
- Sign SAML token for Authentication & Non-repudiation
- Verify expiry & validity of certificates.
- Logout browser session + proper session mgmt.
- XML security

LDAP

→ LDAP is PAM. I AD – LDAP is protocol that allows users to query AD and authenticate access to it.

Light weight Directory Access Protocol

Microsoft AD is LDAP Based like Telephone Directory.

PKI uses LDAP when integrating digital certificates into transmissions. LDAP is the protocol when client query CA for certificate info.

LDAP is centralized Access control system + supports SSO.

Note - simple Authentication & Security layer (SASL) is secure Authentication mode for LDAP.

↳ when we login to AD / Domain controller (DC) which has hierarchical LDAP directory in the database. This database organize network resource & carries out user access control functionality. Upon successful verification to DC, certain network resources are available (printer, email, file server)

LDAP / Open LDAP — is not secure — port 389 — stores user password in clear / unencrypted

LDAP over SSL (LDAPS) — secure — port 636 — secure connection over SSL / TLS

Global catalog services — uses port 3268 & 3269

14. CONTROLING & MONITORING ACCESS

PERSPECTIVE

Permission

Right ↔ Privilege

Access control models

DAC MAC RBAC RUBAC ABAC

Access control Attacks

cove = Authorization methods + Access control Attacks

Understand Authorization Mechanisms

Implement Defense in Depth

Permission + Right = Privilege

Permission: Grant access what can we do with object

Right: Ability to take action on the object

Privilege: Admin have few permission & right on pc data

* Authorization Mechanisms

Implicit Deny
- Firewall
- Everything deny by default until explicitly granted

Access control matrix
- object focused table that includes subjects, objects & assigned Privileges to subjects
- E.g ACL → Focused on objects

Constrained Interface
- Restricts what user can do or see based on privilege
- E.g Executives only see Reports in web BWI

Capability Tables
- Subject Focused
- Table has list of objects that subject can access.

Content-Dependent control
- Restricts access based on content within an object
- E.g Database view (selected columns)

Context-dependent control
- Requires specific activities before granting the access
- Restrict based on date & time

Need-to-know
- based on work tasks & job functions

P.P.O

Least Privilege

- Required privilege + Need to know

Separation of Duties and Responsibilities

- Split sensitive functions into two or more employees
- Prevent fraud

Need-to-know / Access granted to real time b/w 9 to 5

vs.

least privilege / Can read the time + change during PM hours.

ACLs / Access control matrix
↳ Focused on objects

Capability Tables
↳ focused on subjects

Dave may have clearance to access classified data, but access is not granted until Dave's role ~~[illegible]~~ verily requires or need to perform a job.

✱ Defense-in-depth concepts

Administrative controls + technical controls + physical controls

- Security policy + Awareness Training
- FW / IPS-IDS
- Perimeter security

✱ Access Control Models

Revise MAC notes/vedio OSN P633-635

DAC - Discretionary Access control

- Every object has owner / Data custodian
- owner has full control over object to grant or deny access to subjects

RBAC

- Permission based on role / job function / user groups

Attribute Based AC

- More granular/specific than RUBAC
- Use of rules with multiple attributes
- ABAC used by way software-defined networks

Rule Based A C (RUBAC)

- Apply global rules that apply to all subjects (FW)

MAC - Mandatory AC

- Use of labels that applies to objects & subjects
- Top secret user = Top secret Document

✱ Access Control Models : Detailed concepts

Focused on USER IDENTITY

DAC Model = ACL = Object Focused

↳ Data custodian give permission to DAC

DAC ≠ Centrally managed system

because ACLs are easy to modify

↳ DAC is Flexible

To manage central Access control

↳ Non-discretionary AC

- RBAC
- RUBAC
- ABAC
- MAC

Non-DAC model does not focus on user identity. Instead, set of rules govern & manage the Access.

To prevent the Privilege creep — implement Least privilege

RBAC model — helps to implement

MAC model enforce Need-to-know principle using Compartmentalization.

TBAC — Task Based AC — Control Access by assigning tasks, not user identity.

Attribute Based AC (ABAC) — Example — Allow Managers to use WAN from smartphones & Tablets

MAC Model = Lattice-Based Model

Users with sensitive label can access sensitive data

Uses implicit deny philosophy

Also allows label to identify more defined security domains

Adds level of compartmentalization for objects / data

Compartmentalization enforces Need-to-know principle

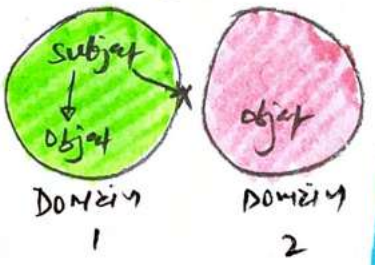
Classification within MAC Model uses three types of Environment:

Hierarchical

- Clearance in one level grant subject access to object in thy level + to all objects in lower level. But, it prohibits access to all objects in higher levels.

Compartmentalized

- Each compartment is isolated environment
- No relation b/w security domains.



Hybrid

- Subject must have clearance + need to know data within specific compartment to gain access to compartmentized object.

MAC is different

Dave = secret clearance

Dave can only access files with secret clearance. Not the ~~lower~~ higher classifications such as ~~sensitive, unclassified~~ top secret

But Dave can access lower - sensitive, unclassified.

NOTE - In MAC model, every subject & object has ~~one~~ one or more labels. Those labels are predefined, and system determines access based on assigned labels.

* ACCESS CONTROL ATTACKS

GOAL

Prevent unauthorised access to objects

Remember? S.T.R.I.D.E

OSCP (31)

Threat Modeling

- identify, understand & categorize potential threats.

identify Attackers

Approaches

- Focus on Assets
- Focus on Attackers
- Focus on software

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- DOS
- Elevation of privilege

From the context of the Attack

- It's important to evaluate the value of Data
- find the Asset valuation

→ this helps to prepare scenario for Attack

Attacks detail P.T.O End

DAC → identity-based AC

RBAC → Role or Group Membership

MAC → Labels to assign access

~~RUAC~~
RUBAC → Rules within ACL

RBAC = Nondiscretionary model + use of hierarchy

Rainbow Attacks — Attackers already have password hashes

Resource based Access controls —
| match permission to resource such as storage
common for cloud-based App

storage X
User A - Read
User B - Read, write

CONFUSION MASTERS — VIDEO

Constrained Interface — Restrictions based on user privilege (Greyed out button) — limited (Many options)

Access control model

Restrict what users can see or do.

RBAC

Least privilege — Provide user rights that requires to finish the job.

Access control concept

MAC

Need-to-know — Limits the access based on whether subject needs to know the information to accomplish assigned task regardless of their clearance

Access control concept

Seperation of Duties — Focusing on preventing fraud or mistakes by spliting task b/w multiple subjects

p.t.o

Video

Constrained Interface — Don't see the clocks on wall

Long (Action) privilege — change time in day / business hours

Need to know (No action) — ~~change~~ Read time for only red clocks

Seperation of Duties — A moves minute hand } 6PM.
B moves small hand