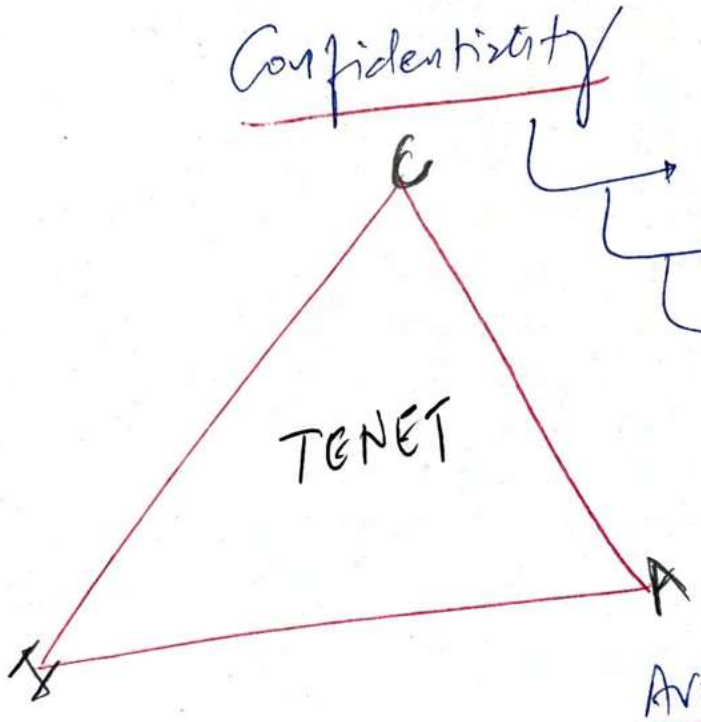
DOMAIN 1

1. Security Governance + Principles + Policies

Confidentiality ⟷ Integrity

Availability $\propto$ Integrity + Confidentiality.



Confidentiality
- At Rest
- Transit
- In use

Availability
- DDoS
- BCP
- log monitoring

Integrity
- Non-repudiation
- Accountability
- 3 Perspectives

Government

1	Confidentiality
2+3	Availability + Integrity

Private

1	Availability
2+3	Confidentiality + Integrity

Security

+

CIA

- Confidentiality
- Integrity
- Availability

AAA

- Identification + Authentication
- Authorization
- Auditing
- Accounting

Non-Repudiation

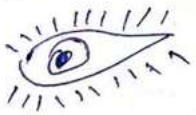
Accounting vs Auditing

Logs

Trails
↳ logs +
user activity

vs

Monitoring



Also
P.t.o sketch at the end

watching logs
(not recording to file)

Possible to monitor without Auditing. But, we can't audit without monitoring.

Something
- Some Do
- You Have
- you know
- you Are

Access control

Subject + object

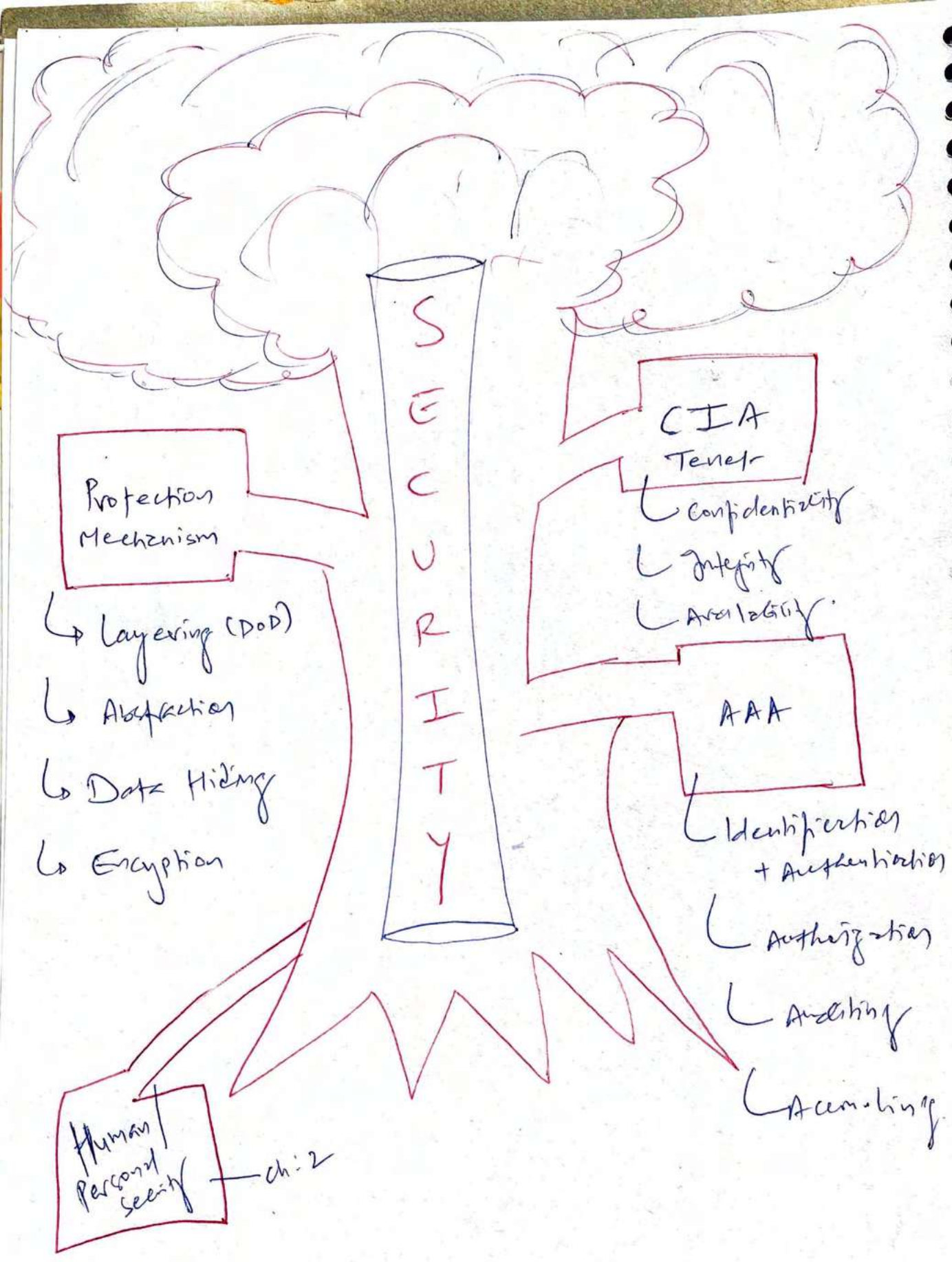
Security control =
counter measures

---→ RBAC

CRITICAL

② Accounting :- Review log files to check compliance & violations in order to hold subjects accountable for their actions.

① Auditing :- Recording log of events and activities related to subjects & objects.


SECURITY
Protection Mechanism
Layering (DoD)
Abstraction
Data Hiding
Encryption
CIA Tenet
Confidentiality
Integrity
Availability
AAA
Identification + Authentication
Authorization
Auditing
Accounting
Human / personnel security
ch: 2

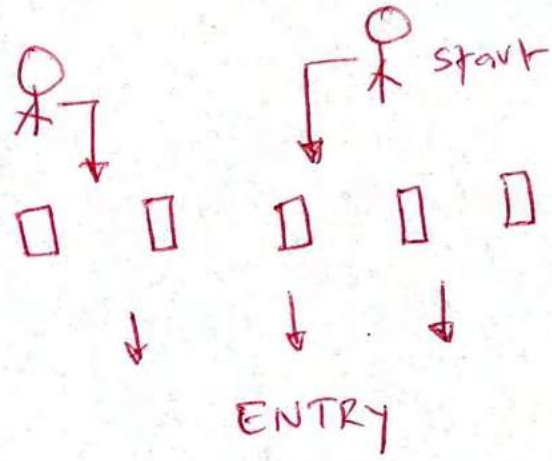
Layering – (Defense of Depth)

Serial config.

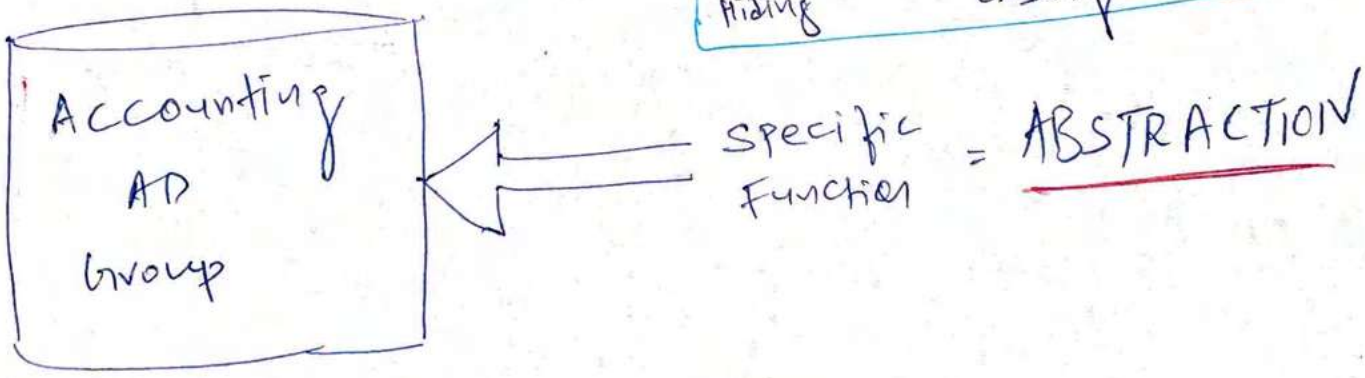
- Immigration

Parallel config.

- Shopping mall



Data Hiding = security through obscurity



Think Encryption

Governance = Vision | Broader Risk

↓

Management = Specific Risk | Planning & Implementation

- Senior mgt ← Security Policy
- Middle mgt [CISO] → Policy, Standards & Guidelines + Procedures

↓

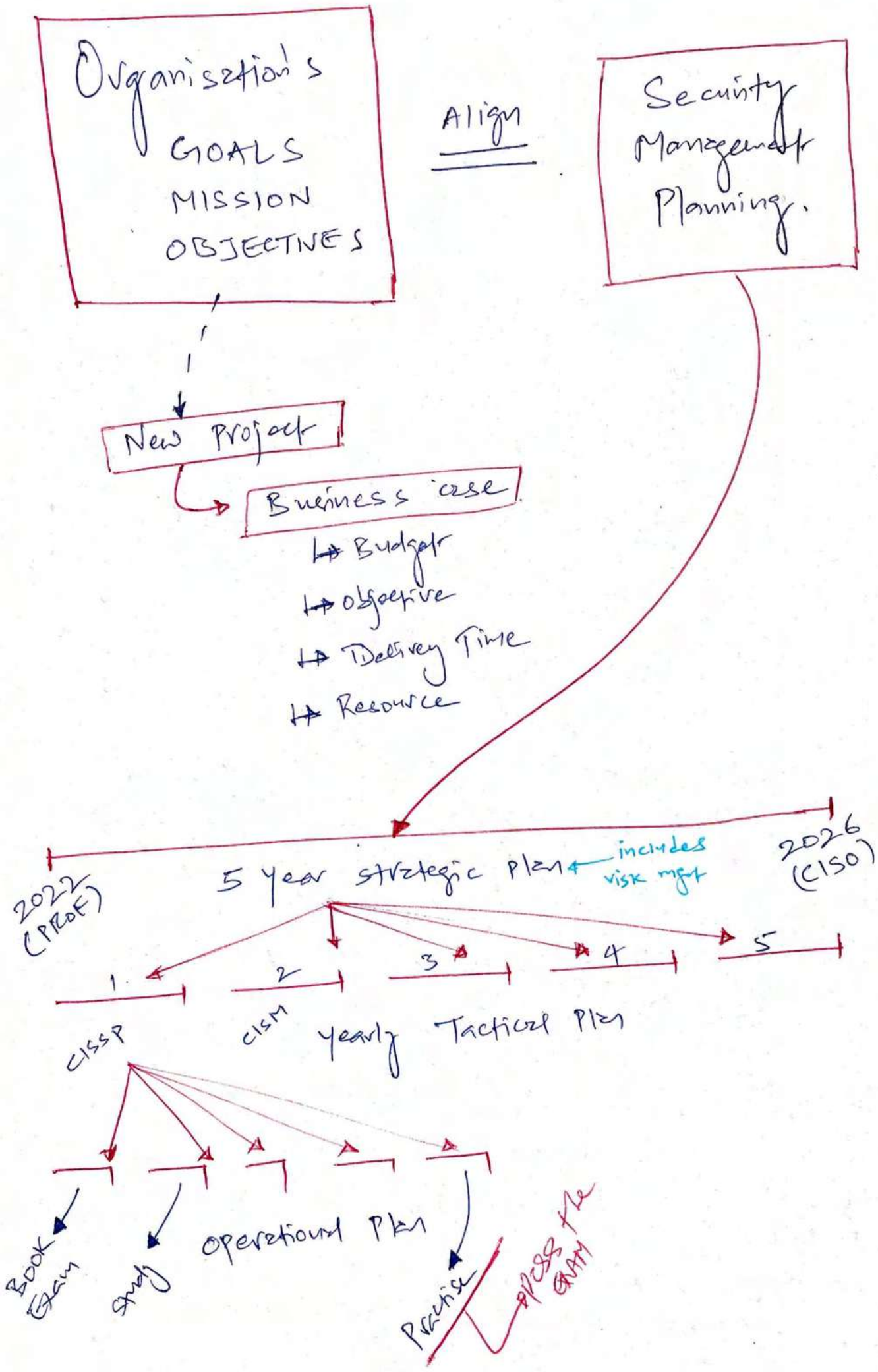
(Operational Managers) Security Professionals ← Assess + implement security controls

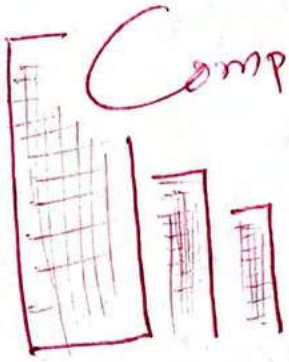
↓

End users ← Comply to security policy + controls

10,000 FT. VIEW

[TOP-DOWN APPROACH]


Organisation's
GOALS
MISSION
OBJECTIVES
Align
Security Management Planning.
New Project
Business case
Budget
objective
Delivery Time
Resource
2022 (PROF)
5 year strategic plan
includes risk mgt
2026 (CISO)
1
2
3
4
5
CISSP
CISM
yearly Tactical Plan
Book Exam
study
operational Plan
Revise
Pass the exam



Company → Acquire, Merge, Divestitures = RISK

PROCESSES To mitigate

Change control mgmt ... CAB ... CIA

↳ To ensure Security is not compromised

↳ To document for auditing

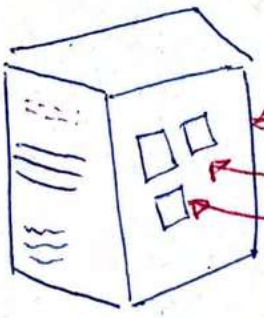
Data classification

Restricted Data ← Give importance

Public Data ← Easy

Declassification

- Equally important



classify physical Asset that holds data — System owner

classify data = Data owner's job

US CAN'T STOP TERRORISM

US — Unclassified, Sensitive

CAN'T — Confidential

STOP — Secret

TERRORISM — Top Secret

Happens before

Anything Valuable

Reasonable care = Due care → Do Correct / involves Actions

Activities to maintain Due care ← Happens After

Due care / involves process / Do Detect → DUE DILIGENCE.

DUE CARE + DD → PROOF TO RISK MGMT

SECURITY INFRASTRUCTURE

(5) (Mandatory) PROCEDURES — system / sw specific

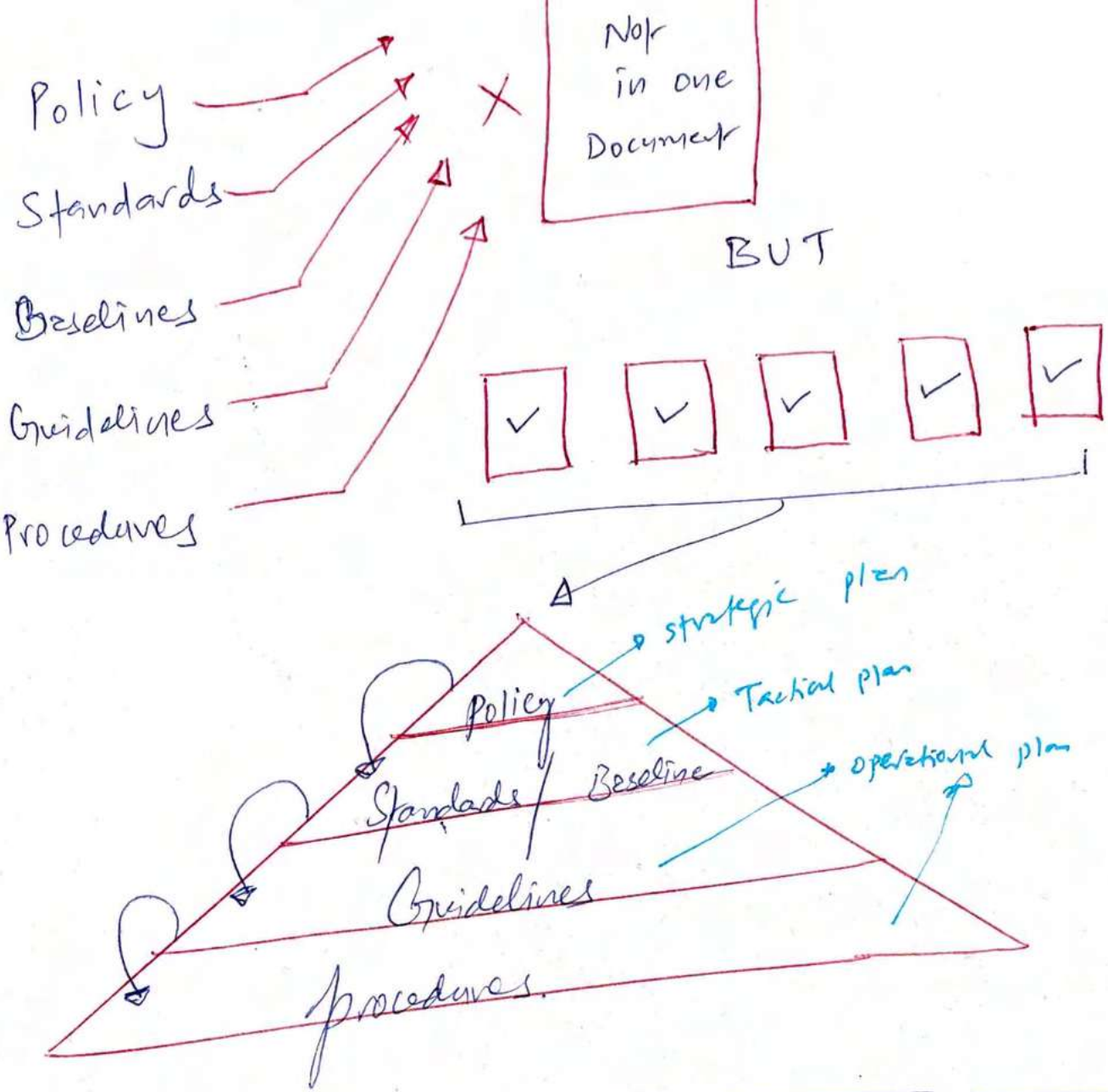
(1) (Mandatory) POLICY — Strategic plan → 10,000 ft. of Security Roadmap

(2) (Man.) STANDARDS — Tactical plan → Security Roadmap Implementation

(3) (optional) BASELINE ~~PROCEDURES~~ — Minimum Security Requirements → NIST, PCIDSS, CIS — System Specific

(4) (optional) GUIDELINES — implementation guide for standards & ~~Procedures~~ Baseline

Operational Plan



IDENTIFY → CATEGORIZE → ANALYZE → MITIGATE → RESPOND

Threat Modeling ⇒ Reduce Risk

→ 2 Approaches

Proactive / Defensive → SAST

Reactive / Adversarial → DAST

START (Non-Prod) → SYSTEM DESIGN → FINISH (Prod)

Pen Test

Fuzz Test

APPROCHES

Threat Modeling

1. → Proactive / Defensive
2. → Reactive / Adversarial

(IDENTIFY) Identifying Threats

1. → Focus on Assets — Valuations — Implement Access controls
2. → Focus on Applications / softwares
3. → Focus on Attackers's Goals

Understand ETHICAL HACKING

Consider OWASP TOP 10 — OAP

(CATEGORIZE)

SOFTWARE FOCUSED ← Microsoft's

STRIDE threat model methodology

- S – Spoofing — why not called "Social Engineering"
- T – Tampering
- R – Repudiation
- I – Information Disclosure
- D – DDoS
- E – Elevation of Privileges

(CATEGORIZE)

Threat Model Methodologies

- **STRIDE**
  - To assess threats against
    - OS
    - Applications
- **DREAD** (for Response P.T.O)
  - based on 5 questions
    - Damage
    - Reproducibility
    - exploitability
    - Affected Users
    - Discoverability
- **PASTA**
  - For Asset Protection
- **TRIKE**
  - Open source.
  - Accepted Risk level for each class of Asset
- **VAST**
  - For Agile Project Mgmt.

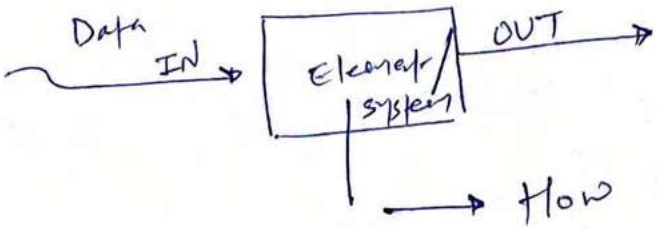
(ANALYZE) = Data Flow Diagram

Define

- Protocol
- Technology
- Application
- OS
- Environment

Think each with STRIDE Perspective

Threat Reduction (MITIGATE) = Decompose or Dissection



THINK!

→ How Data is entered
→ What happens to Data inside the element
→ How Data is stored?
→ How Data is secured inside the element?
→ How Data is coming out?

threat reduction / decomposition process

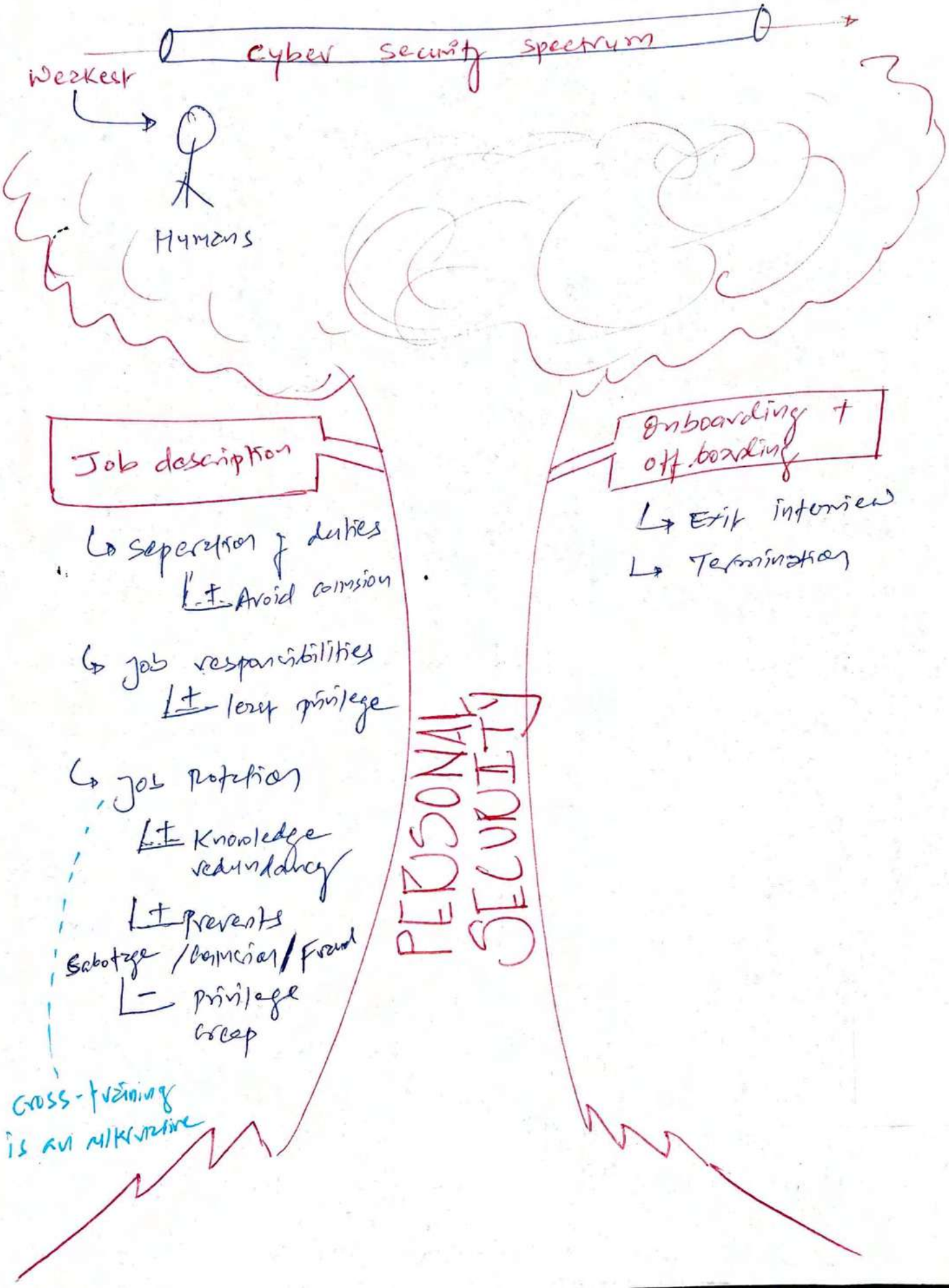
1. Trust Boundaries = VPCSC
2. Data Flow Path - movement & data flow locations
3. Input Points - location where external input is received
4. Privileged Operations = SA / Admin A/Cs.
   → cyberARC (PAM)
5. Security stance & Approval = Align with sec. policy.

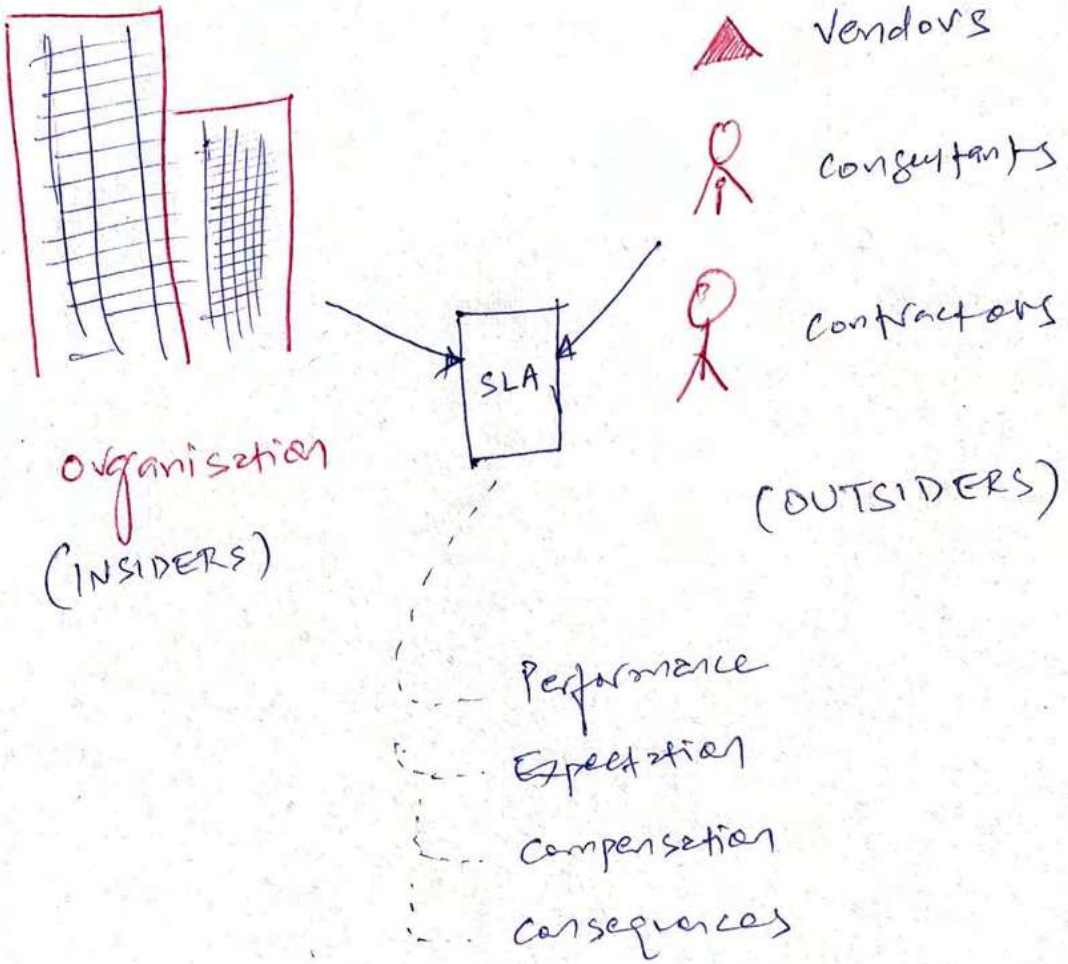
REDUCTION ANALYSIS

(RESPOND) — D R E A D

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability.

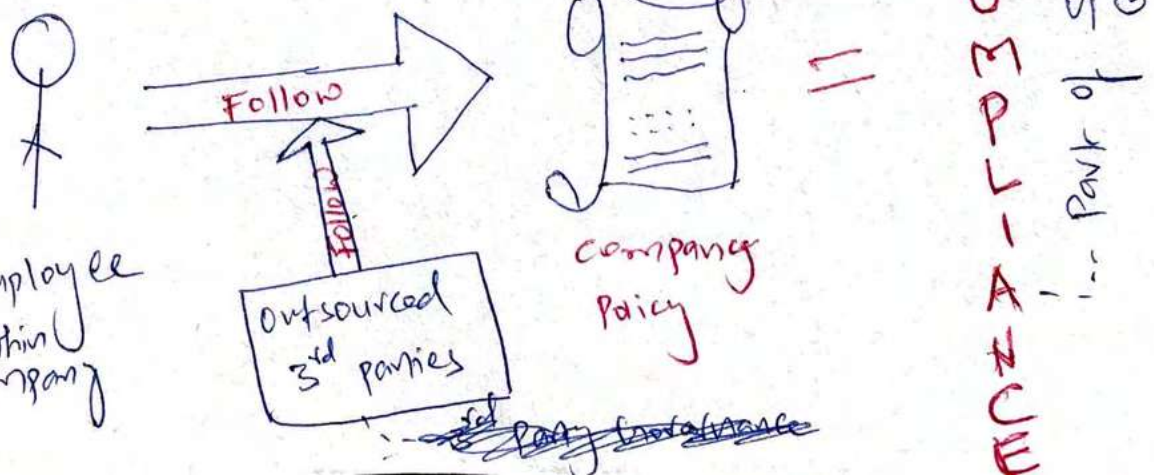
2. Personal Security + Risk Mgt.



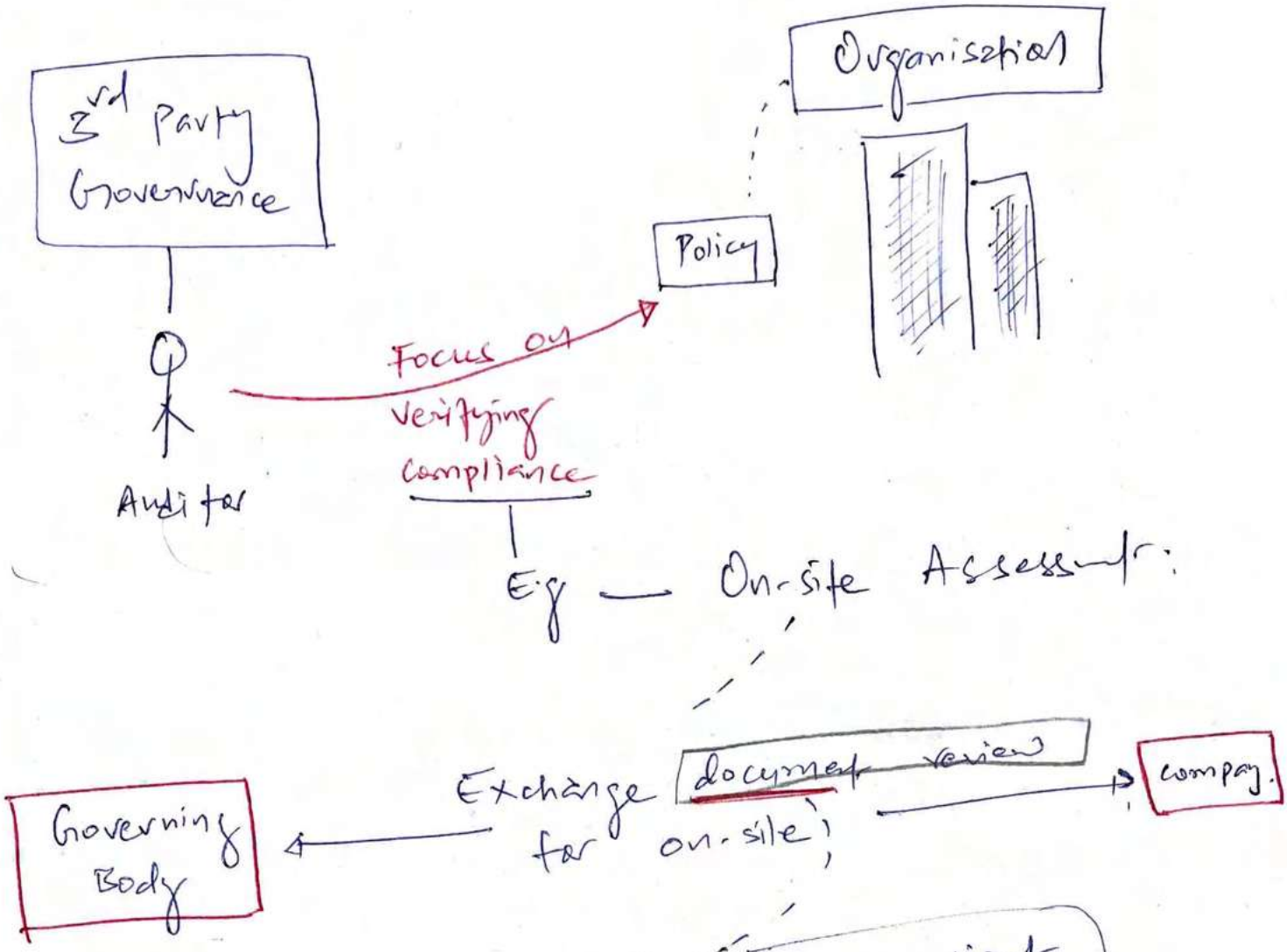


Name
Address
Mobile
Passport

PII Data ⟹ Need PRIVACY POLICY



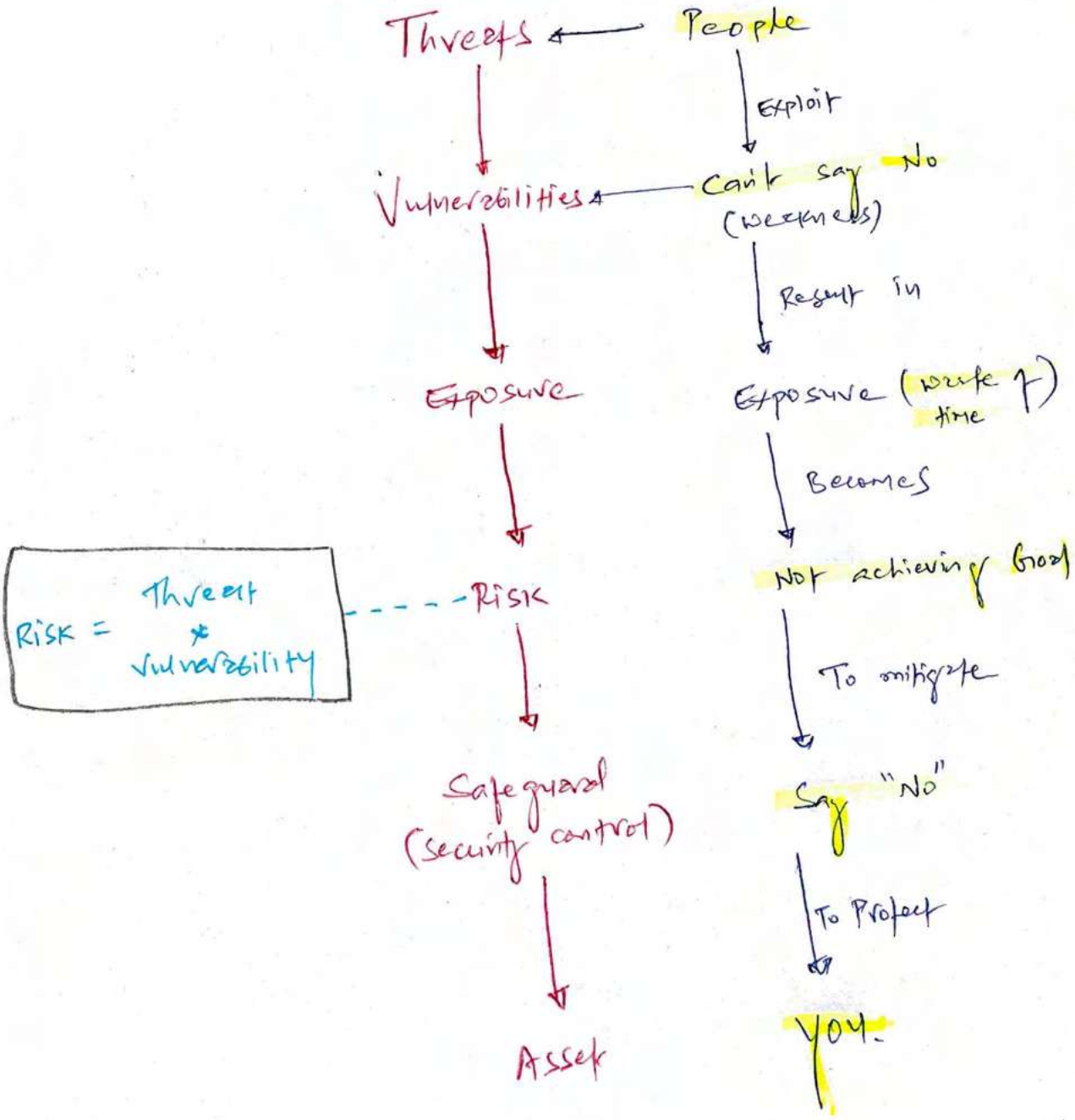
~~3rd Party Involvement~~



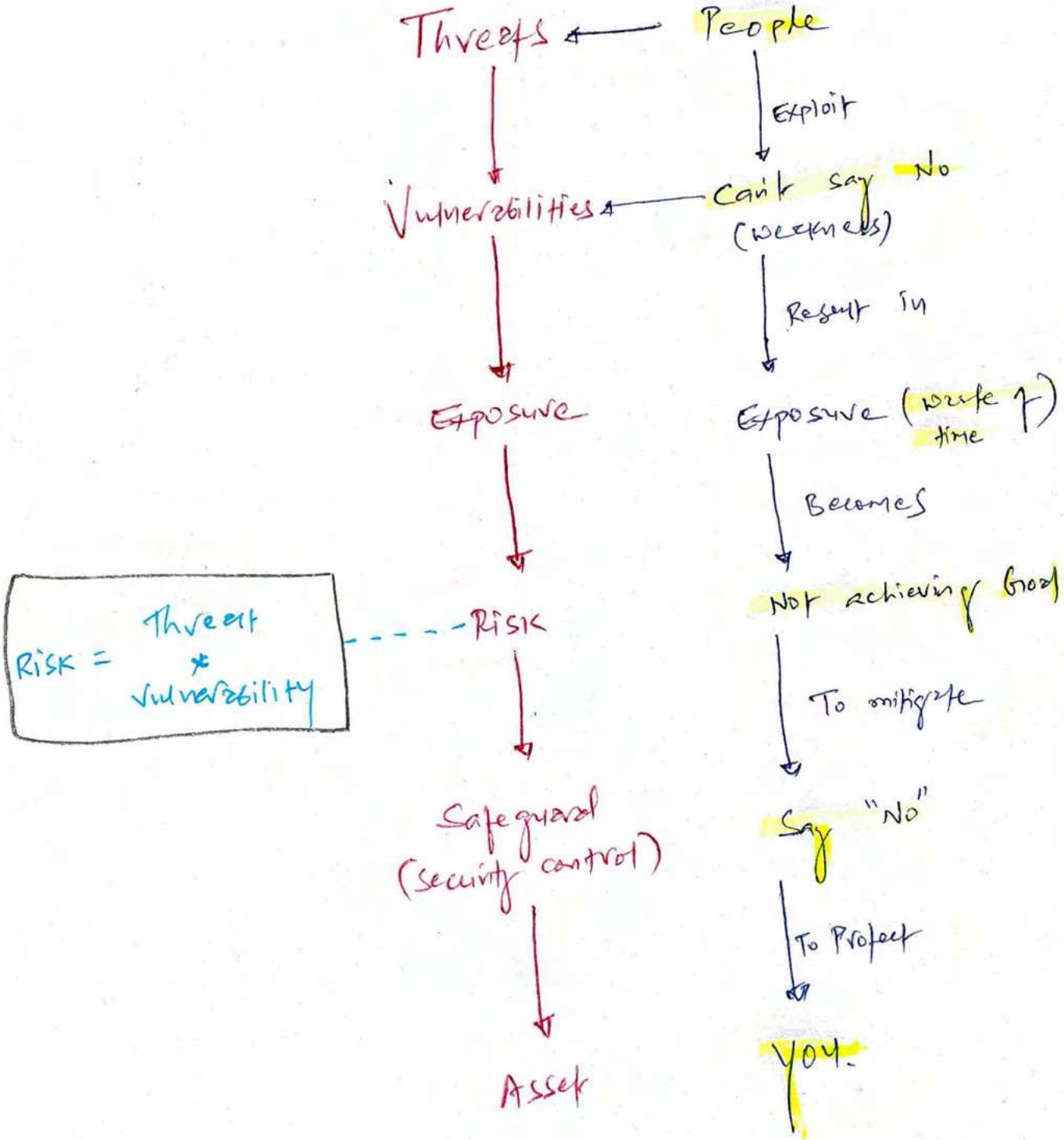
Loss of Authorization to Operate (ATO)

- once ATO is lost or revoked, a complete documentation review & on-site review showing full compliance is necessary to reestablish the ATO.

RISK MANAGEMENT
CONCEPTS



RISK MANAGEMENT
CONCEPTS



Risk Management

→ Primary goal: To reduce the risk to acceptable level.

1 **Identify**
- Threats
- Vulnerabilities

2 **Analysis / Assessment**
- P.T.O END: 6 STEPS OF RISK ANALYSIS
- Quantative (P.T.O End (more notes))
  - EF
  - AV
  - SLE
  - ARO
  - ALE
  - ACS
- Qualitative
  - Delphi technique
- ALE = SLE * ARO
  - SLE = AV * EF
- Safeguard Evaluation
  - (Pre-ALE) − (Post-ALE) − ACS

3 **Response**
- $200 SPEED FINE
- Mitigate / implement security controls. (max speed 60.)
- Assignment / Transfer to friend.
- Accept (A.K.A Risk Appetite) (Risk tolerance) — pay fine — when cost/benefit analysis has negative value
- Deterrence (60) - speed sign
- Avoidance / Find alternate route
- Risk Rejection (P.T.O)

ignoring risk that exists — driving Around / Smoky

Risk Rejection

Residual Risk

This is Mgmt chose to accept the risk rather than to mitigate.

Total Risk

Threat * Vulnerabilities * Asset Value

Total Risk – Controls Gap

Countermeasure / Security control

Refer to Risk Mitigation.

4.

3. Physical.

2. Technical / Logical

ASSET

(Data)

1. Administrative

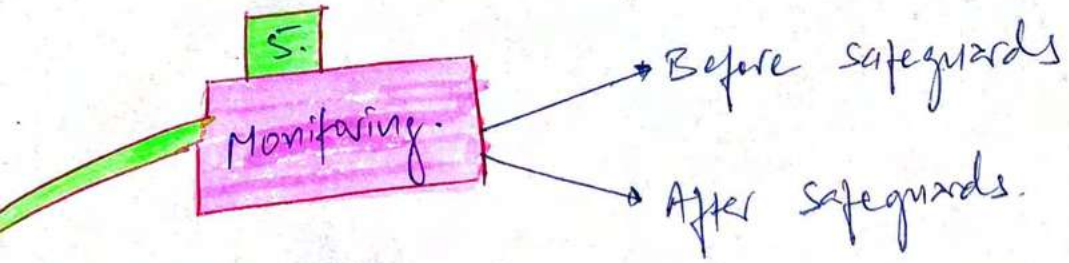
SECURITY CONTROL MAIN CATEGORIES.

other controls. P.T.O.

Applicable Types of controls.

1. Deterrent → Physical
2. Preventive → physical + technical.
   - Firewall
   - Pen Test
   - Fencing
   - IPS
   - Data classification
   - Least privilege
   - Sec. Awareness training.
3. Detective → 

4. Compensating → defense in depth
5. Corrective
   - virus → Quarantine → Fixed.
6. Recovery
   - RAID
   - Backup & Restore
   - BCP
     - Backup & Restore
     - Hot / warm / cold sites
7. Directive
   - Force system to complain → EXIT SIGN.
   - SIEM – monitoring



RMF - RISK MANAGEMENT FRAMEWORK

NIST 800-37

7 STEPS.

with 2 PERSPECTIVE

NIST 800-53

Information System

1. Prepare
2. Categorize
6. Authorize

Security Control

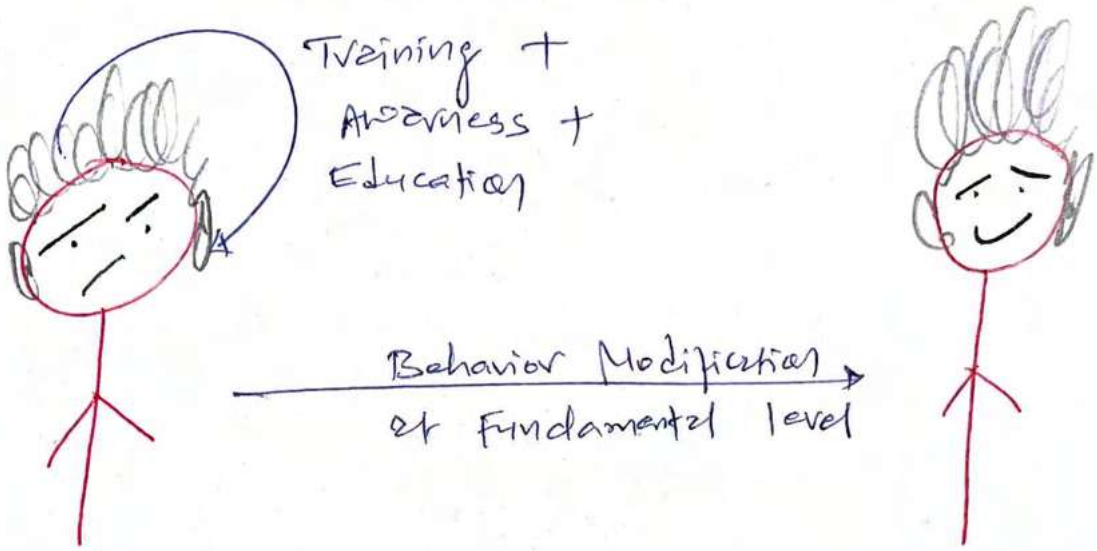
3. Select
4. Implement
5. Assess
7. Monitor

People can See I Am Always Monitoring.

CISSP = NIST 800-37 RMF

Other RMFs

- OCTAVE
- TARA
- FAIR



Perform
Risk Assessment

SECURITY FUNCTION → SHOULD BE

COST-EFFECTIVE

AV = $10K

Safeguard = $5K

Profit = $5K

MEASURABLE

Pre-safeguard
50% RISK

Post-safeguard
20% RISK.

QUANTATIVE
* RISK ANALYSIS STEPS :

① Inventory Assets — find AV. (Asset value)
$200K

② Identify Threats — calculate EF & SLE
50%

SLE = AV * EF
= 200 X 50%
= 100K

③ Perform Threat Analysis — calculate the likelihood of vertical threat (ARO) = 10%. (0.10)

10 | 1 / 10 / 10 — 1 in every 10 year

④ Estimate the potential loss — ALE = SLE * ARO
100 * 0.10
= $10K

⑤ Research countermeasures for each threat.
— security controls to reduce risk

ALE1 − ALE2 − ACS (Annual maintenance cost) = True value safeguard

⑥ Perform cost/benefit Analysis
— For each countermeasures for each threat for each asset.

Total Safeguard value should not exceed more than $10K.

Risk = threat * Vulnerability

↖ This is absolute

Exposure = is a possibility

- low exposure can result to high risk
- high exposure can result to low risk

Safeguards

- Not only purchasing new products
- Reconfigure existing elements
- Removing elements from Infra.

Attack Vs Breach

Intentional attempt to exploit vulnerability

when security mechanism is bypassed ↘ Backdoor

if bullet still hit with body armour, you still die

=

if safeguard fails, the loss of Asset is same as there is no safeguard.

3. Business Continuity Planning

BCM
BCP
DR

SHOW MUST GO ON FOR COMPANY

BCP: Focus on Business operation
- Takes care of overall Energy
- Strategic (long term)
- 10,000 ft high-level
- Business mgmt related

DR: Focus on IT Activities ----- ch: 18
- Tactical (short term)
- Micro-level.
- IT related
- Takes care Immediate emergency

BCP PROCESS 4 STEPS

1. Project Scope & Planning
   - Business organization Analysis
   - BCP Team selection
   - Resource Requirements
     - BCP development
     - BCP Testing, training & maintenance
     - BCP Implementation
   - Legal & Regulatory Requirements

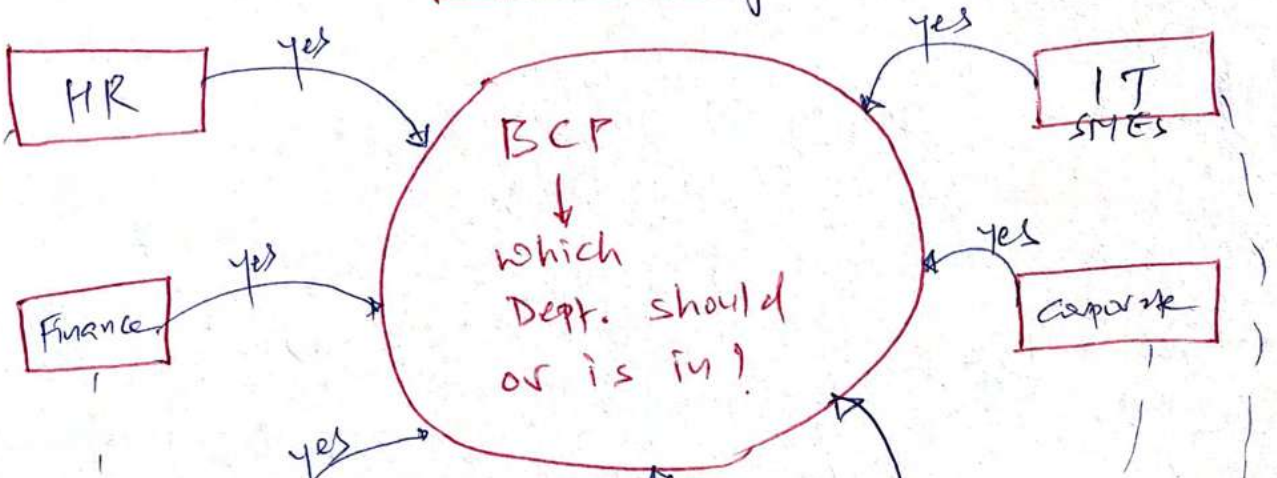
2. Business Impact Assessment (BIA)
   - Analysis
     - (A) - Qualitative Decision making
     - (B) - Qualitative Decision making.
   - (1) Identify Priorities
   - (2) Risk Identification
   - (3) Likehood Assessment
   - (4) Impact Assessment
   - (5) Resource prioritization

3. Continuity Planning

4. Approval & Implementation

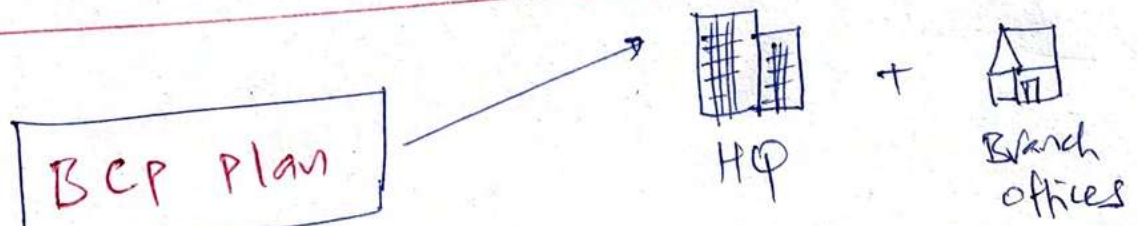
pp.0 Evaluation -1

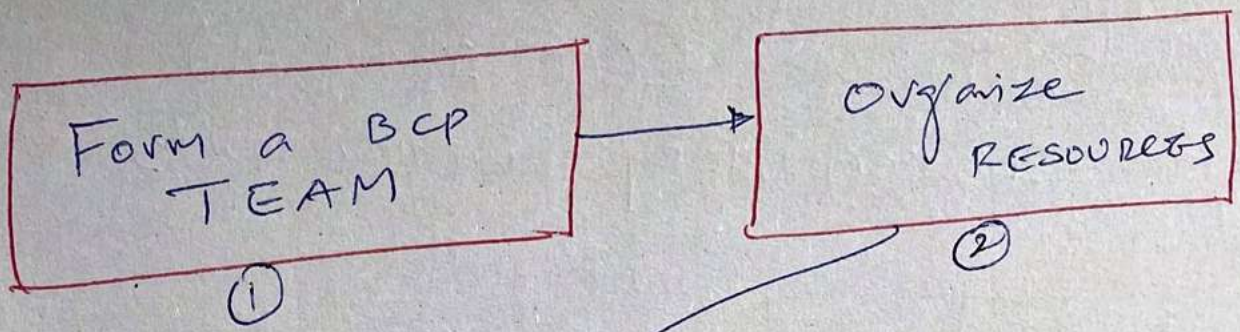
1 | BCP | Project Scope & Planning



1 Person from Each Department who is responsible for functional core business service

= BCP SQUAD / TEAM





3 Phases

1. **BCP Development**
   - ↳ mostly BCP team members
2. **BCP Testing, Training & Maintenance**
   - ↳ H/W + S/W commitments
   - ↳ Employees involved into BCP.
3. **BCP Implementation**
   - ↳ Requires significant resources
   - ↳ Prepare to fight with senior mgmt to get more resources with BCP business cases.

Mgmt don't want to invest $$ for BCP?
Ask this question —
How long seat-of-the-pants recovery might take when compare to orderly, planned continuity of operations

SEAT-OF-THE-PANTS ATTITUDE

$1M

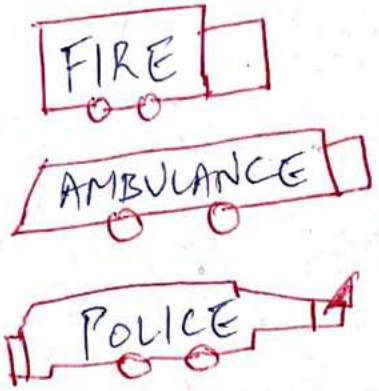
vs

BCP

$200K

→ consider disaster business cost & indirect cost of lost opportunities.

ENFORCE BCP AS LAW + REGULATORY REQUIREMENTS

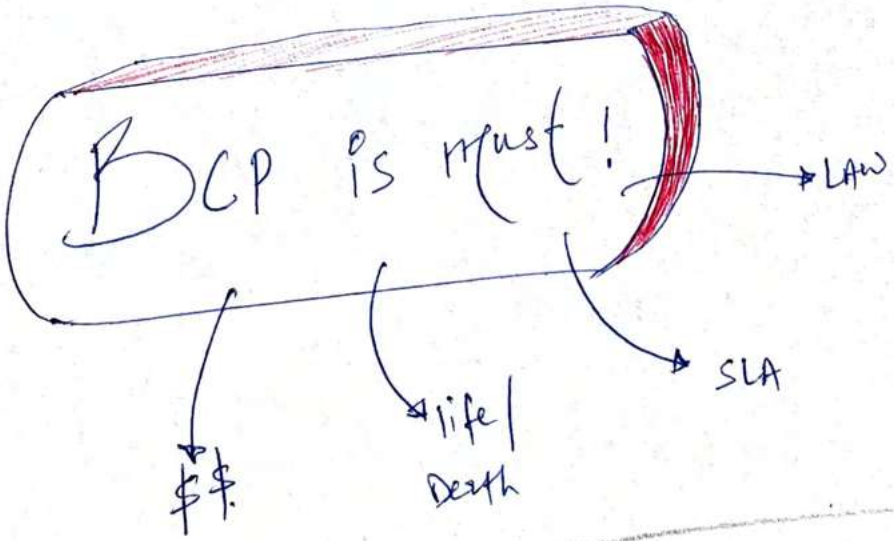


BCP = LIFE OR DEATH.

BCP = Contractual obligation / SLA from customers.

(w/ 3 parties)

BCP Promises → Win NEW clients $ $$$



Get BCP policy Documented & get a formal approval from the management.

2 | BCP | BIA

STEP-1 , Business Impact Analysis STEP-2 = HEART , STEP-3 → p.t.o

YOU ARE HERE

STEP-5 ← p.t.o , STEP-4 → p.t.o

Analysis

Quantative (Numbers + Formula + $$ figures)

Qualitative (scenario + intuition + experience)

~~plan~~ ~~create~~ ~~tests~~

Decision

WHAT IS BIA ANYWAY ??

↑ BIA identifies RESOURCES that are critical to organization, also threats to those RESOURCES, & likelihood of impact those threats on business

Data loss tolerance = defined back up strategy

RPO = Recovery of Data

p.t.o for DIY/WIFE SKETCH

NETFLIX IS DOWN

MTD / MTO
- Maximum Tolerable Downtime or outage

2 hours

RTO = Recovery of mission critical process
- Recovery Time Objective

1 hour

MTD > RTO — should be

BIA PROCESS

4 p/o

5 p/o +2

1 Identify Priorities
- Quantitive measure
- with MTD & RTO
- Netflix Example (← p.t.o)

2 Risk Identification
- Qualitative in nature
- Natural Risks
- Man-made Risks

3 Likelihood Assessment
- ARO

USGS
- US Geological survey
- FREE RISK REPORTS

JAPAN'S EARTHQUAKE
- 5-6 / year
- ⇓
- ARO
- Annualized Rate of occurance

organization + Insurance company = Risk transfer

⇓

Perform Risk Assessment = MUTUAL BENEFIT.

SPIN-OFF (side note)

BIA for cloud = SOC

Service Organization control

Form of Assessment → [SOC Report]

cloud vendor → Provide

✗ SOC 1 → only internal control / descriptions

✓ SOC 2/3 → Security, Privacy, Availability controls

4 MOST CRITICAL STEP

Impact Assessment

FEED ①

3. Identified Risks +

4. Likelihood

② Produce overall Business Impact.

Quantitive Perspective

AV

EF

SLE

ALE

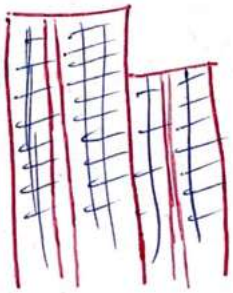
ARO

ARO = likelihood

Eg Five 1 in 30 year

$$30 \overline{)100} \quad 0.03$$

ARO = 0.03%.



BUILDING

$500K

AV = Asset value

one Five = 70% Damage

EF = Exposure Factore

Single time loss due to Five

→ SLE

$$SLE = AV * EF$$

$$= \$500K * 70\%$$

$$SLE = \$350K$$

Five occurs once every 30 years

ARO = 1/30

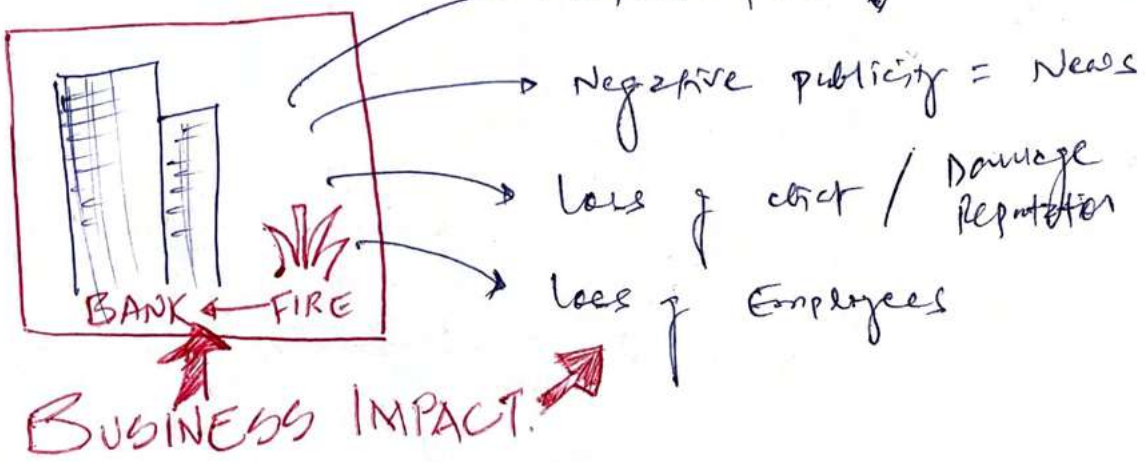
= 0.03

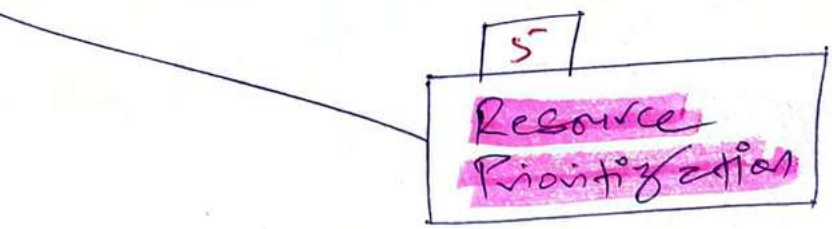
$$ALE = SLE * ARO$$

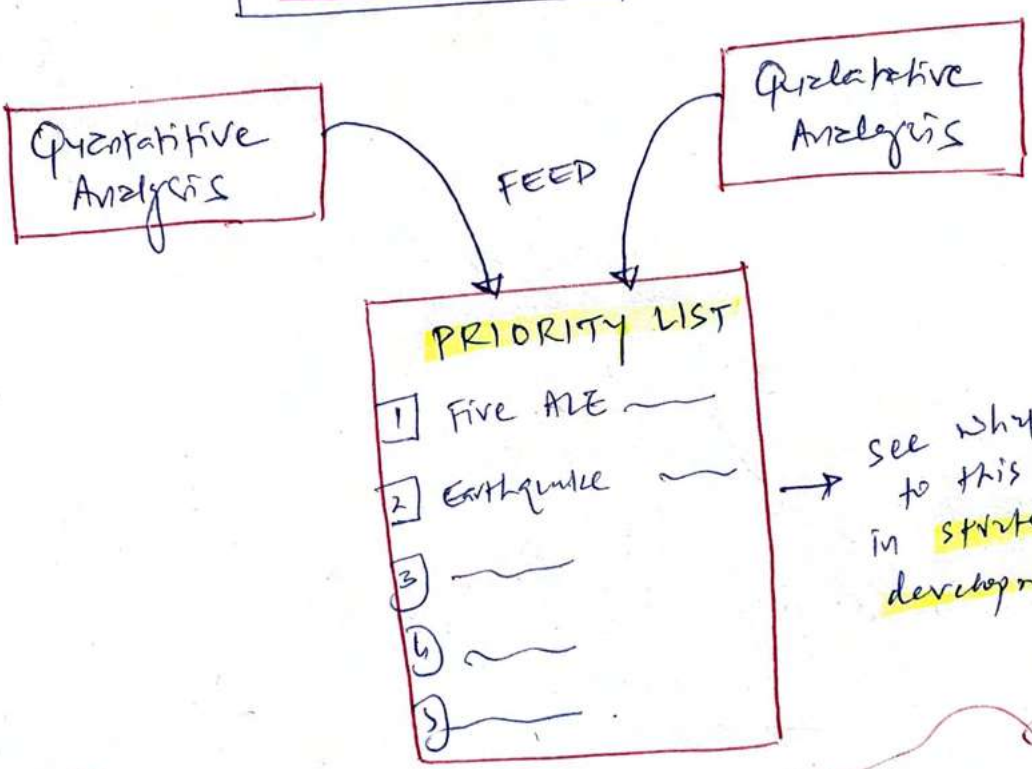
$$= \$350K * 0.03$$

$$= \$10,500$$

Annualized Loss Expectancy - Business can expect loss of $10,500 every year due to fire in building.







~~(BCP PROCESS - TREE SO FAR~~

BCP PROCESS

Project Scope & planning

BIA

1

2

3 Continuity Planning

4 Approval & Implementation

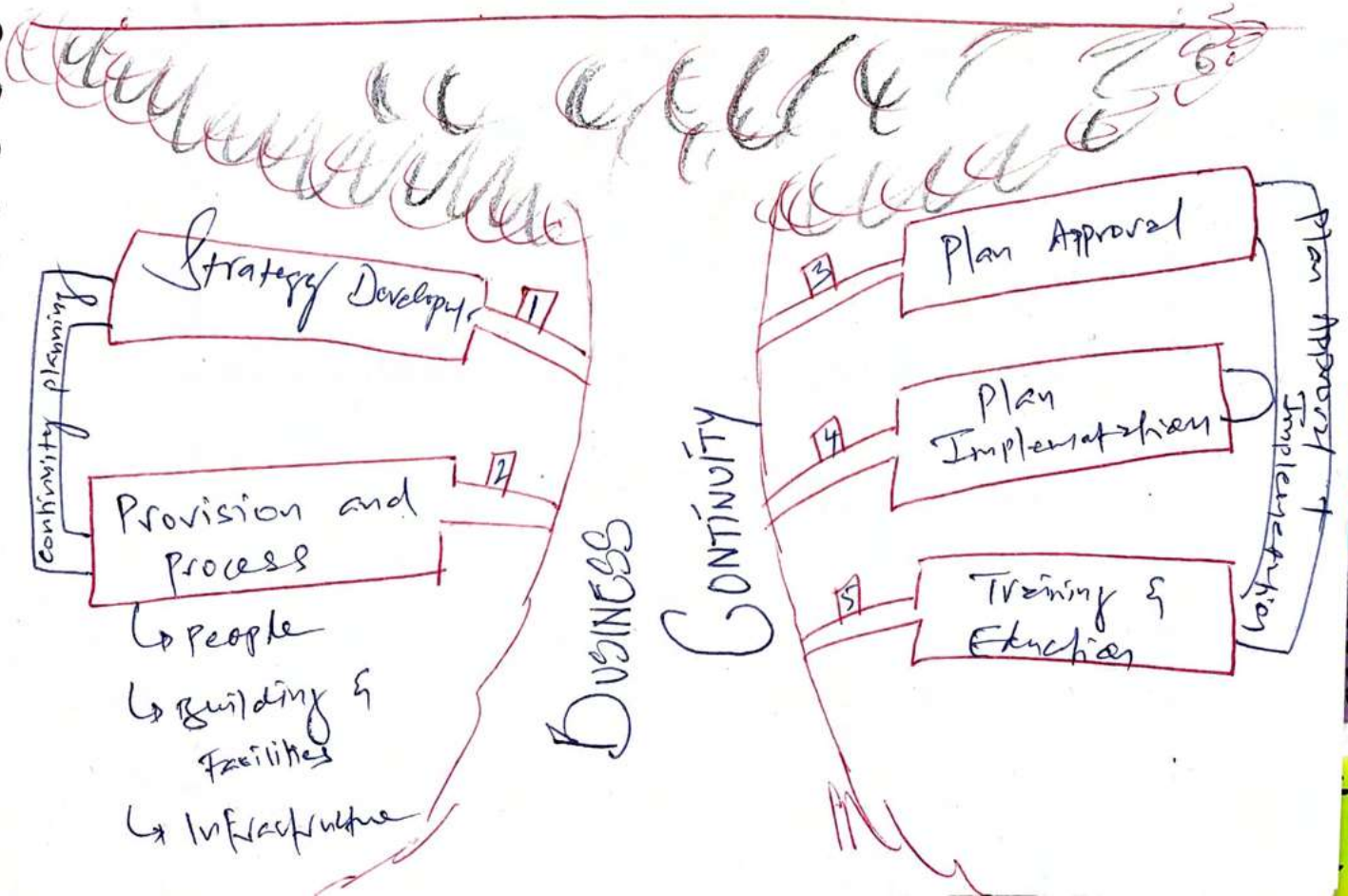
3	BCP	CONTINUITY PLANNING

1. Project planning
2. BIA

FOCUS —
- How BCP Process will work
- BCP speed
- What are the Priority Business Asset in case of interruption.

FOCUS 1

- Whatever impact we realized from (1) & (2)
  - → How BCP strategy will be DEVELOPED + IMPLEMENTED.



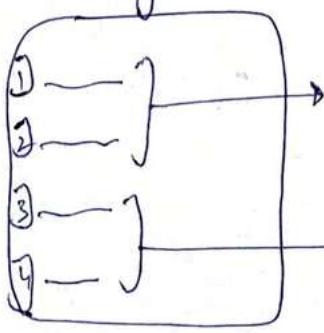
1. STRATEGY DEVELOPMENT

BIA — STRATEGY DEVEL. — CONTINUITY PLANNING PHASE

BRIDGE

BIA's step (5)

Priority list



Risk Accepted = No Problem

Risk to be mitigated

- Who will mitigate? (Resource)
- How it will mitigate? (Plan + implementation)

Feed into Next step

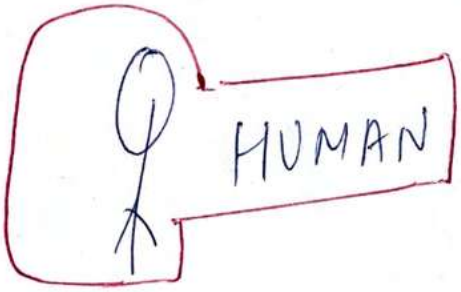
2. PROVISION & PROCESSES

Because this is where we mitigate

→ MEAT OF BCP

Saves 3 types of ASSETS

1. People
2. Building & Facilities
3. Infrastructure



HUMAN = MOST VALUABLE ASSET

Building Facilities

- Hardening Provisions → Existing site → Fix leaky roof
- Alternate site → if Existing site hardening fails.

Hot, Cold, Warm sites

Infrastructure

→ Physical Hardening

- UPS x Racks
- Fire Alarms
- sprinklers

Alternate Systems

Redundancy ---- Availability

DC1 Sydney

DC2 Melb.

4	BCP Plan Approval + Implementation

Business continuity planning

5	BCP

BRIDGE

1	BCP
2	

GET APPROVAL FROM SENIOR MGMT.

(1) Plan Approval

Try to get endorsed by top executive such as CEO for BCP importance + WEIGHT

(2) Plan Implementation

↳ Deploy BCP resources

(3) Training & Education

↳ BCP resource

↳ Backup resource

(4) BCP Documentation

↳ Event / Emergency

↳ Historic records

Important components of BCP

1. Statement of Importance
   - Signed by BCP Lead, CEO = weight
   - BCP Lead, lower mgt = Resistance
   - Signal why BCP is important! with CEO signature
2. Statement of Priorities → Priority list from BIA
   - critical Business Functions in order of priority for continue operation
3. Statement of Organization Responsibility → can be incorated to Statement of Importance
   - SENTIMENT: BCP IS EVERYONE'S RESPONSIBILITY.
4. Statement of Urgency & Timing
   - outlines implementation of timetable
   - shows why BCP is critical.
5. Risk Assessment → All that Formulas + Maths.
6. Risk Acceptance / Mitigation
   - RISK → Accepted = reason?
   - RISK → Unaccepted = Security control

ASK BUSINESS LEADER A QUESTION

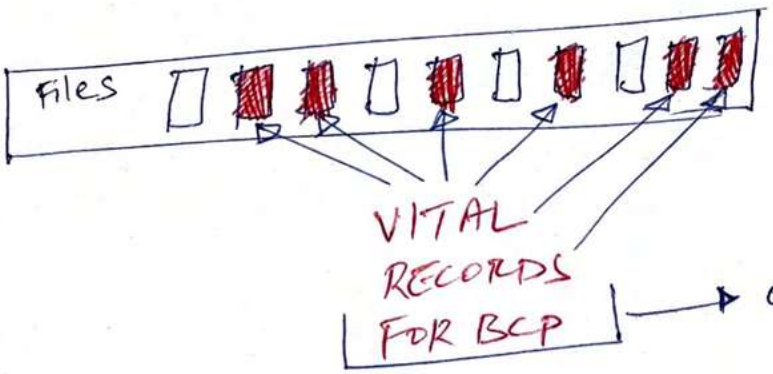
Why Risk is accepted!
(residual risk)

7 Vital Records Program

→ what records you need if we have to rebuild the organization in new location without accessing computers?

↳ How to retriere Docs | Records in Disester!

↳ where is it stored!



→ ORGANISE FOR EASY FIND!

8 Maintainance

↳ Living Document for BCP
↳ Periodic update
↳ version control
↳ Destroy old versions.

It's good practise to include BCP components in job descriptions, so it remains fresh.

9 Emergy - Response Guidelines

↳ New employee should be able respond to emergency situation
↳ immediate response procedures
↳ whom to contact / notified of the incident
↳ secondary response procedures.

Emergency guidelines should be easily accessible to employee in the organization

10 Testing & Exercise

--- chap: 18

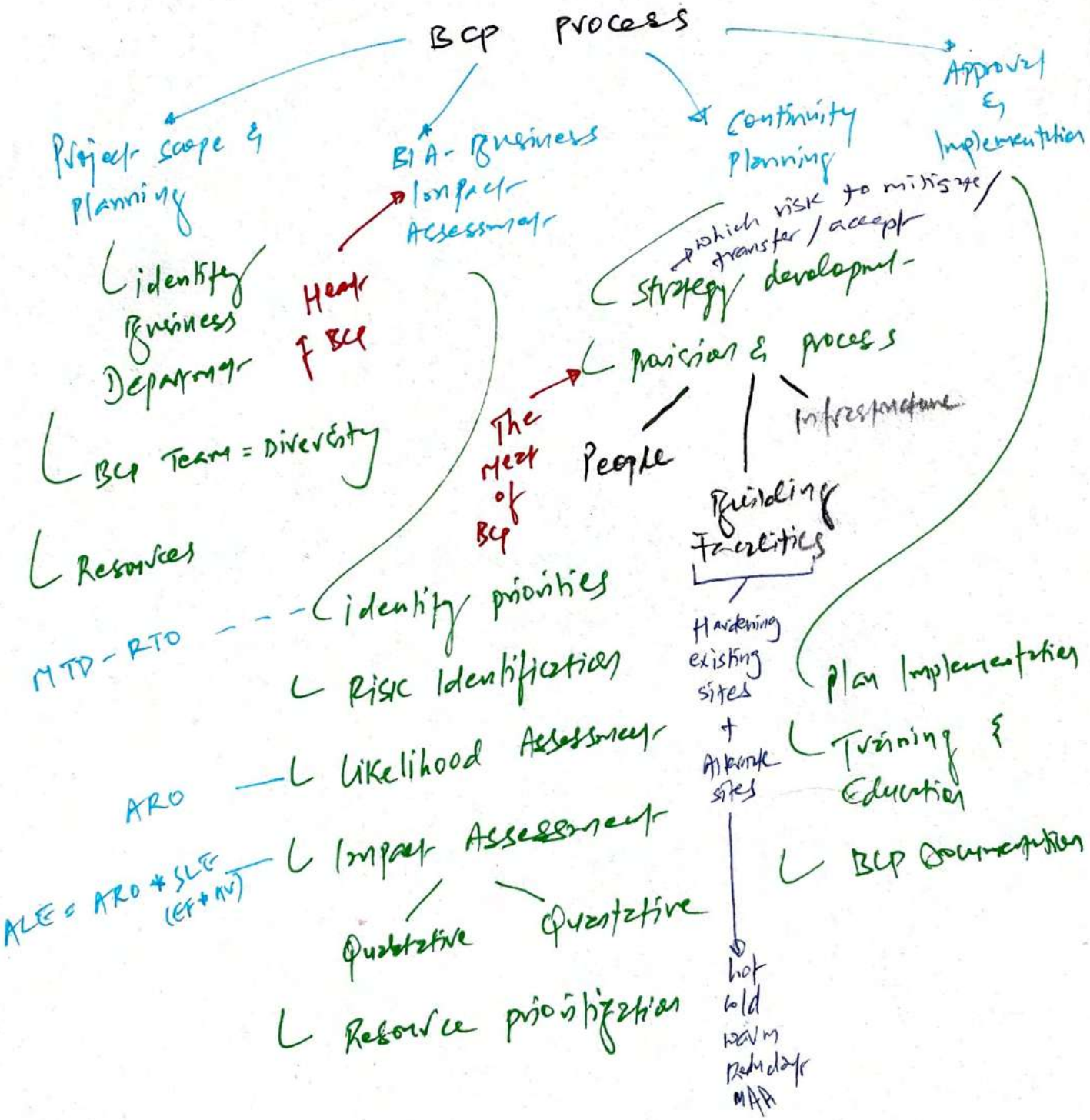
BCP doc to ensure that personnels are trained to perform their duties in the event of disaster.

Slowing down continuity process will blow MTD!!

BCP / DRP Planning High level steps

Blueprint

BCP/DRP Ultimate Goal – To restore normal business operations after disaster struck using effective and secure strategies.



BCP / DR → Deals with → Availability of CIA Triad

You really need a BCP coordinator who would liaise with employees, mgmt

Business Impact Analysis is different than Risk Analysis

Identify critical business process & functions & assign criticality score to those processes

↳ if router is down, what's the MTD? what's the RTO? Before business losing $$$

identify Assets & assign criticality or risk score

↳ Router has higher Risk score than desktop computer

BIA's two exclusive thoughts

→ if it doesn't happen, that doesn't mean we can't plan for it.

→ if it most likely won't happen, that doesn't mean we can't assign the risk score. just assign the lower risk score
Eg (>100M file must be scanned for malware = top vine)

location, location, location

Mantra Real Estate

Document, Document, Document

IT mantra

BIA General steps

- Who is going to be interviewed / (Identify stakeholders)?
- What techniques to gather data?
  - Q&A / interview
  - Quantative + Qualitative Analysis
- What are Business critical functions?
  - Amazon APP - products (Netflix) — movie portal
- What critical resources each critical function requires?
  - Front End UI

How long each critical functions survive without critical resources?

- Without Web UI, how impact will be for Amazon (Netflix)

What are the THREATS to these critical Functions?

- Hack
- DDoS
- Misconfiguration
- Human Error / mistake

Amazon (Netflix) Front UI = Mission critical

Assign MTD rating to each critical Function (Business)

Document & Submit to Senior management.

THIS IS LUKE AHMED'S BIA PERSPECTIVE

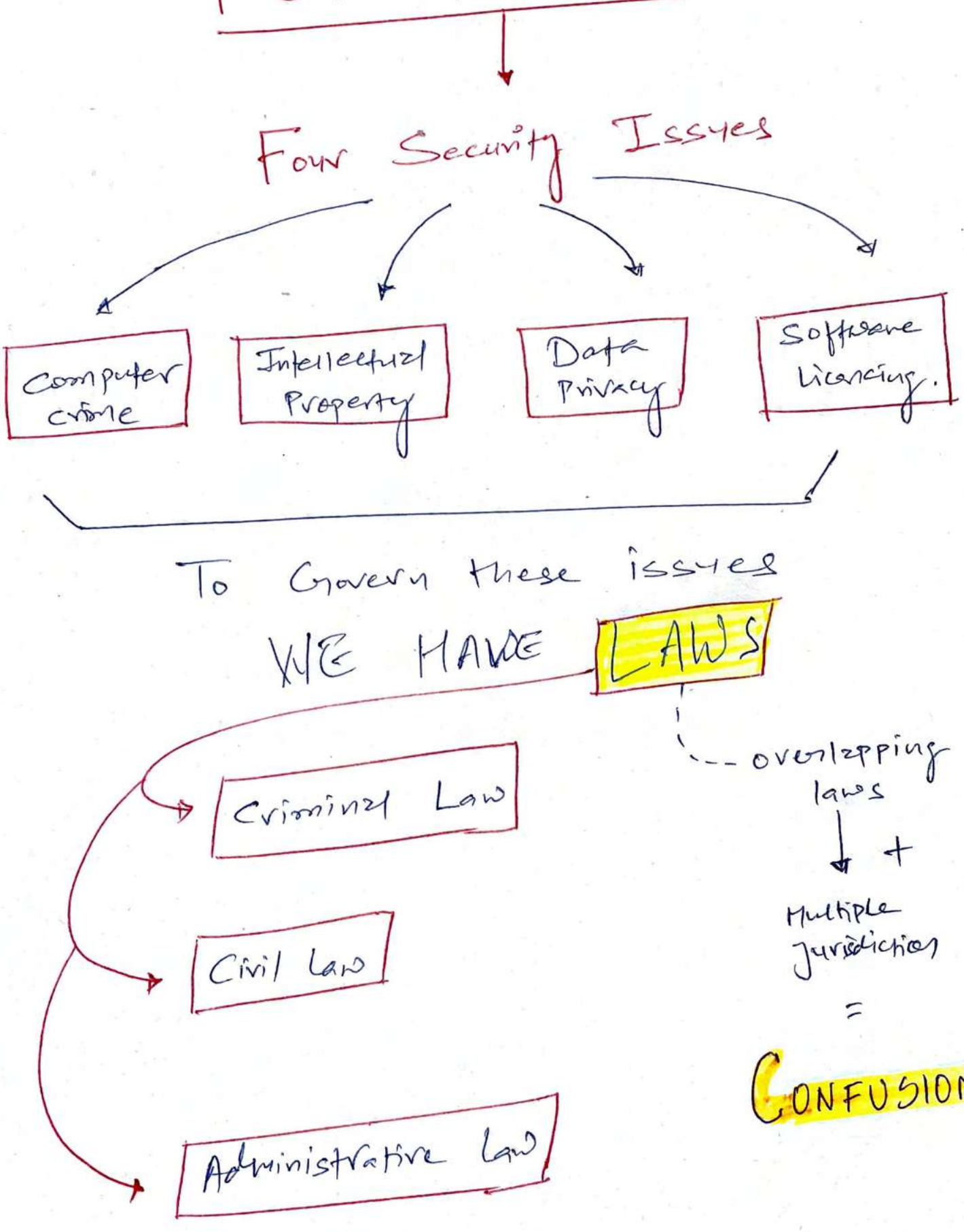
BCP DEVELOPMENT PROCESS

1. Develop BCP Policy statement (RMF Prepare)
   - High-level executive direction on what BCP accomplish + required resources
2. Conduct BIA
   - How to mitigate & their associated cost (below :-)
3. Identify Preventive Controls (above :-) NIST-800-53
   - Identify critical business process + function (MTD, RTO, RPO, WRT)
4. Develop Recovery strategies — IT staff develop DRP
   - How IT service will be restored in order of priority. This includes
5. Develop an IT contigency plan
6. Perform DRP testing & training
   - Test DRP to ensure method + identify Gaps.
7. Perform BCP / DRP maintenance. (RMF Phase 6)
   - Review BCP & DRP process every three months
   - Audit annually.

Developmt of BCP starts from these steps.

4. Laws, Regulations, & Compliance

PERSPECTIVE



CRIMINAL LAW

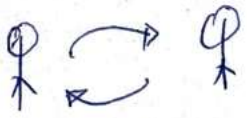
100%.
Federal + state government

- Computer fraud
- Abuse Act
- Electronic & comms. privacy Act
- Identity Theft
- Digital Millennium copyright

CIVIL LAW

Min. Govt involvement

Transaction



People

organization

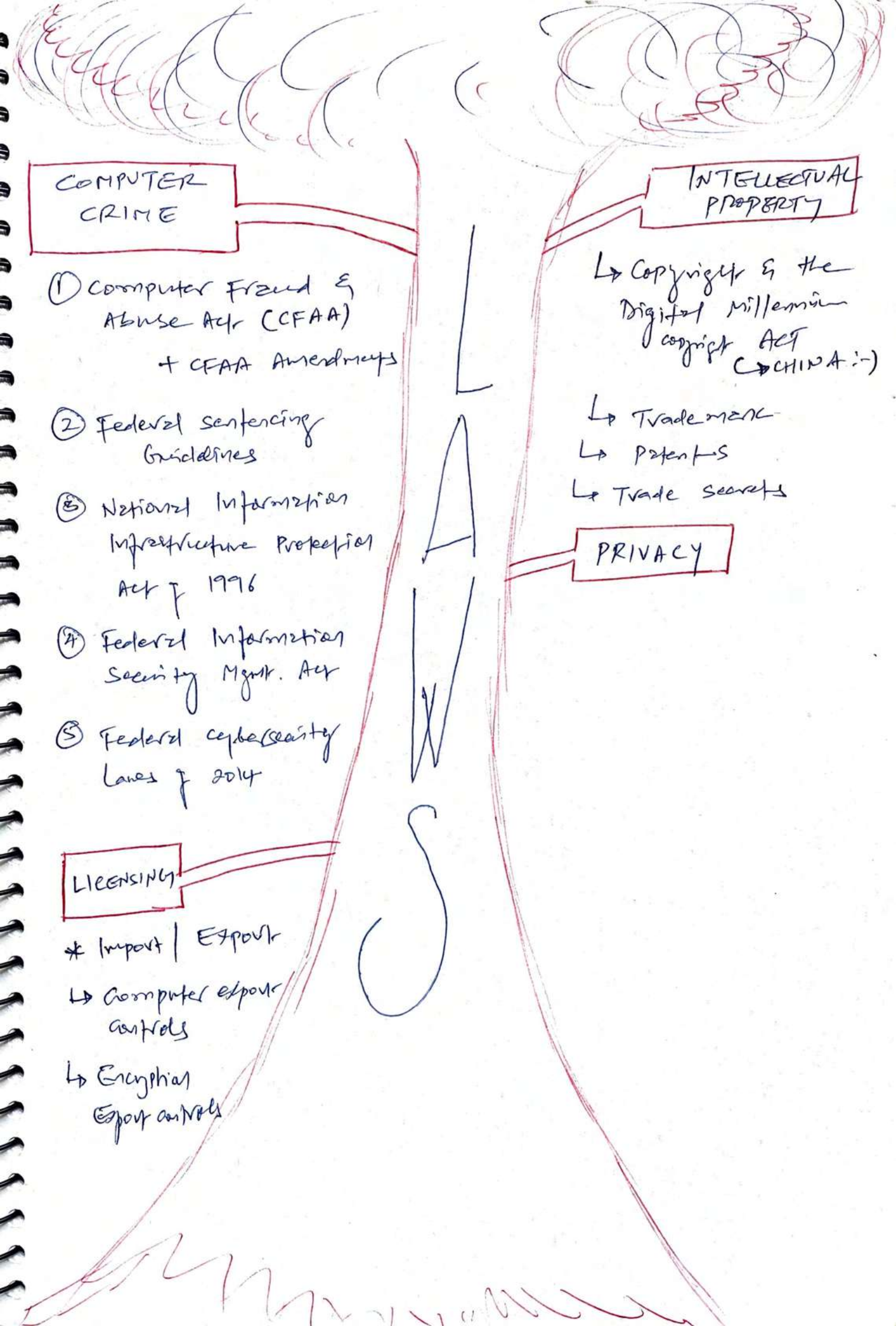
- Trademark
- Patent laws

Branch

Administrative Law

Government Agencies

- Day to day activities
- HIPPA: / Specific industry + Data Types


COMPUTER CRIME
1) Computer Fraud & Abuse Act (CFAA) + CFAA Amendments
2) Federal sentencing Guidelines
3) National Information Infrastructure Protection Act of 1996
4) Federal Information Security Mgmt. Act
5) Federal cybersecurity Laws of 2014
LICENSING
* Import | Export
↳ Computer export controls
↳ Encryption Export controls
INTELLECTUAL PROPERTY
↳ Copyright & the Digital Millennium copyright ACT
↳ CHINA :-)
↳ Trademark
↳ Patents
↳ Trade secrets
PRIVACY
L
A
W
S

Copyright

Protects the original work of Art

Protects the work, not the creator

Trademark

Name, slogan, logo

Patent

Protection of creators of new inventions

protects the creator

(right to obtain a patent)

Trade secret

protects the operating law of firms

Digital Millenium copyright Act of 1998

- prohibits copy protection mechanism placed in digital media + limits the liability of ISP for activities of their users

Economic Espionage Act of 1996

- Penalty to individuals who found guilty of the theft of trade secret

(if it's a benefit of foreign govern)

Licensing

- Contractual
- Shrink-wrap
- Click-Through
- Cloud Services

NOTES FROM Q&A

Multi-factor Authentication

- Something you know
  - Password
  - PIN
  - Security question
- Something you ARE
  - Fingerprint
- Something you have
- Somewhere you are

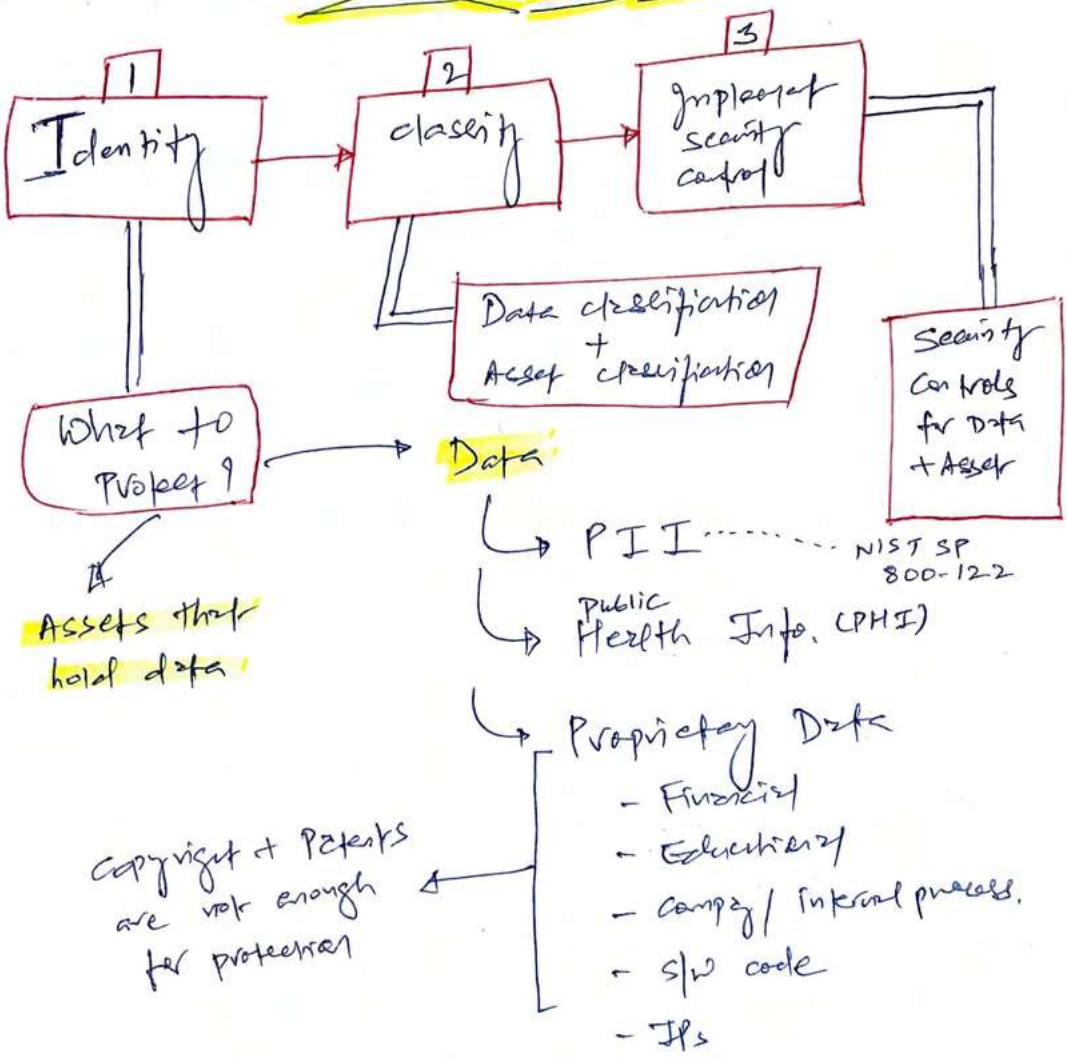
Note :- True MFA is the one when we use technique from each category (Password + Fingerprint)

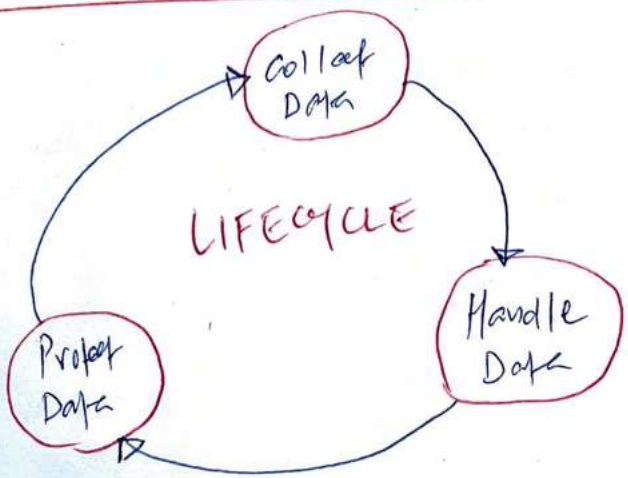
To licence manifacturing process to other companies

- Patent
  - ✓ Suitable
- Trade secret
  - ✗ only appropriate when details can be tightly controlled within organization

DOMAIN 2

5. PROTECTING SECURITY OF ASSETS





DATA ----- 2 QUESTIONS

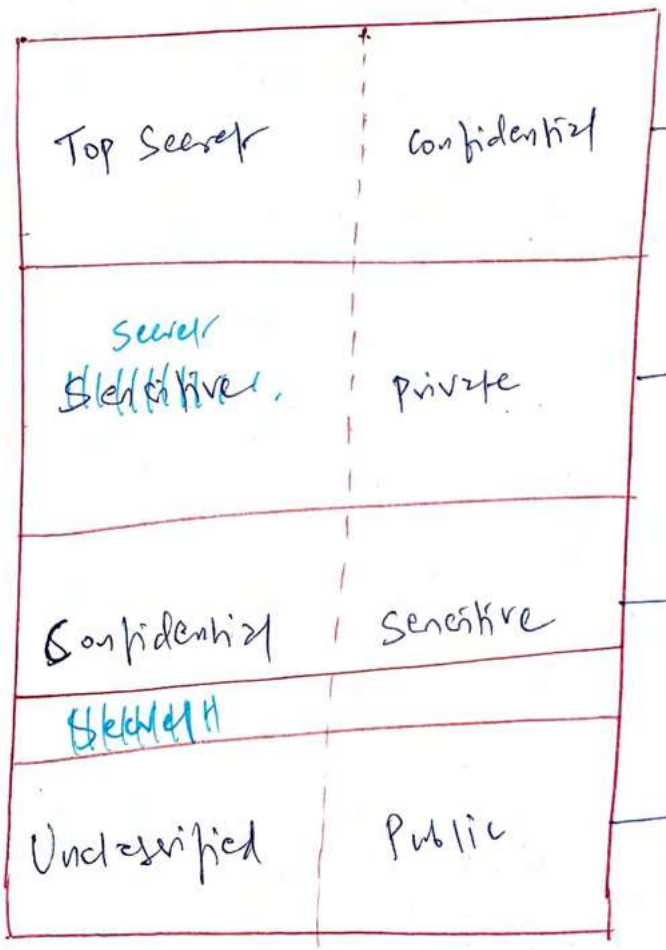
How sensitive is the Data ?

How critical is the Data

Defines the classification

Defines the consequence if Data lost

US CAN STOP TERRORISM

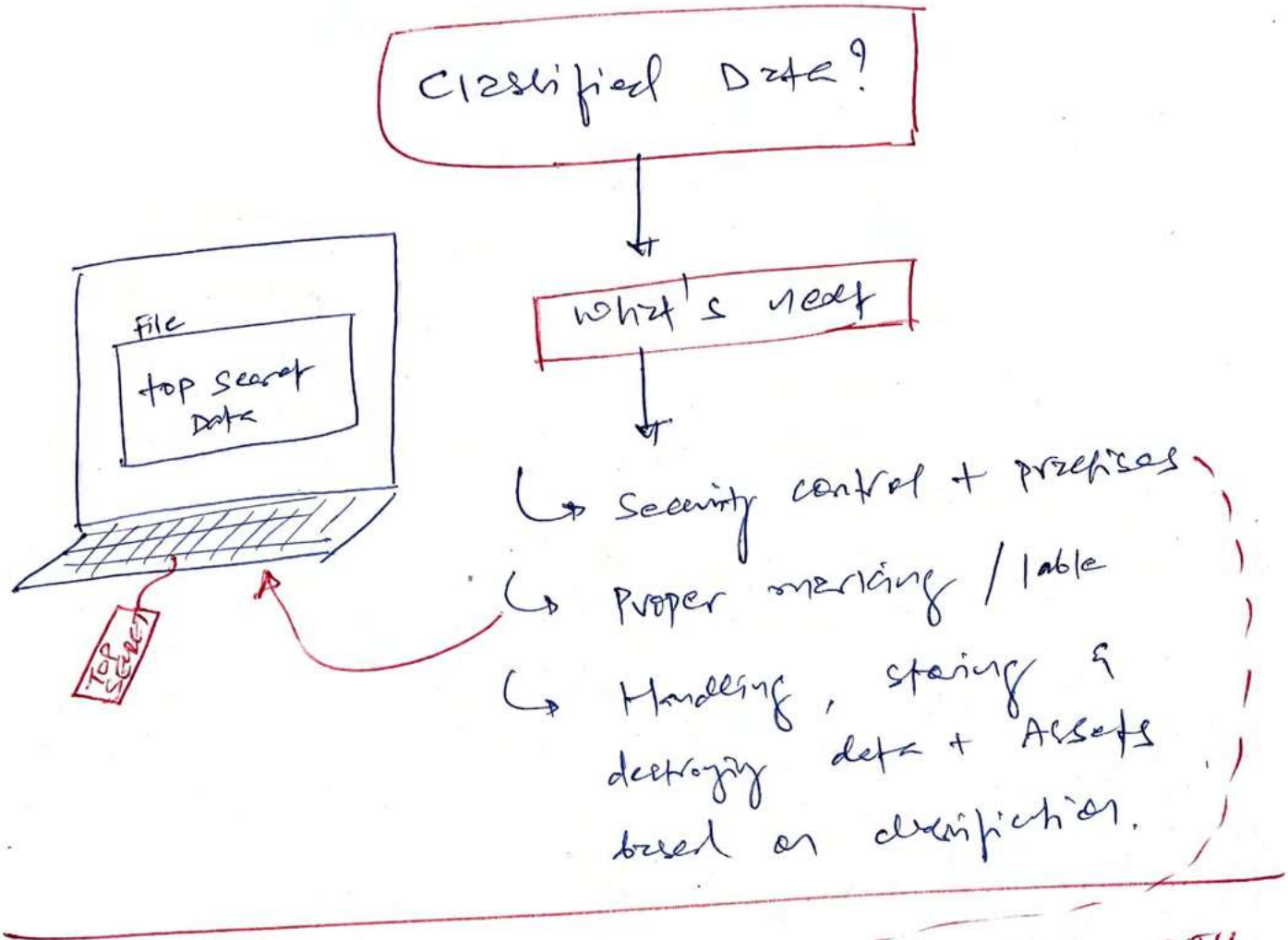


$1B marvel Leak movie = Severe Damage

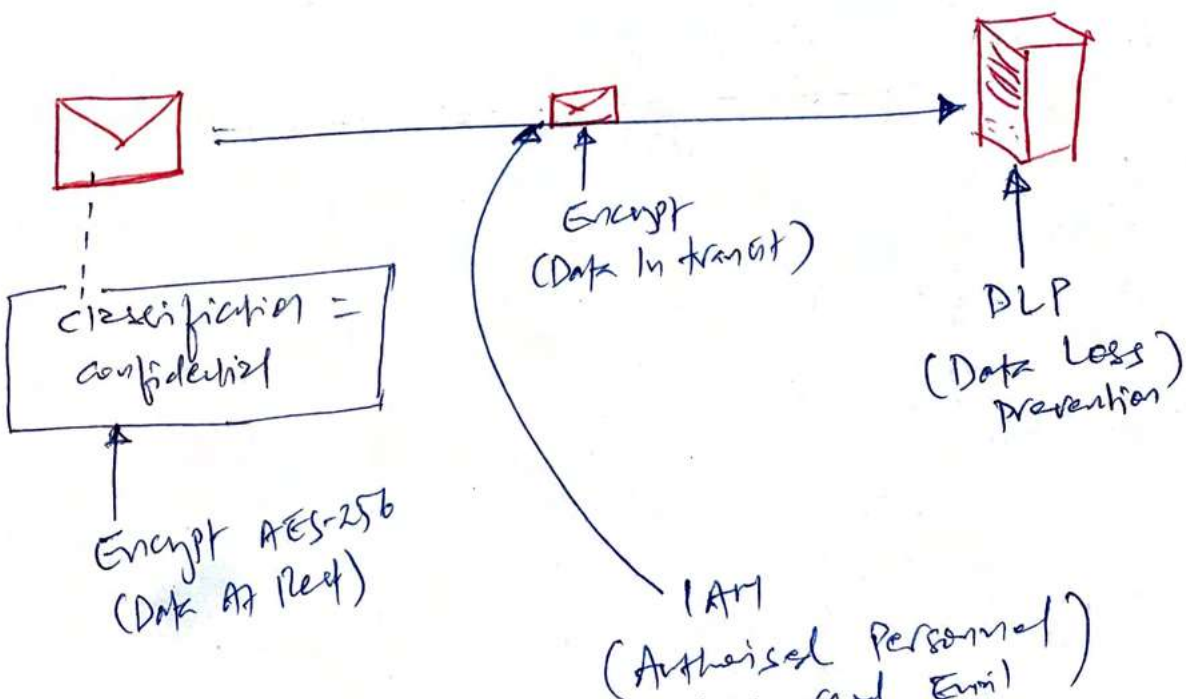
Serious damage = Payroll data breach

Damage = Any technical / non-technical data breach that makes official's job easy.

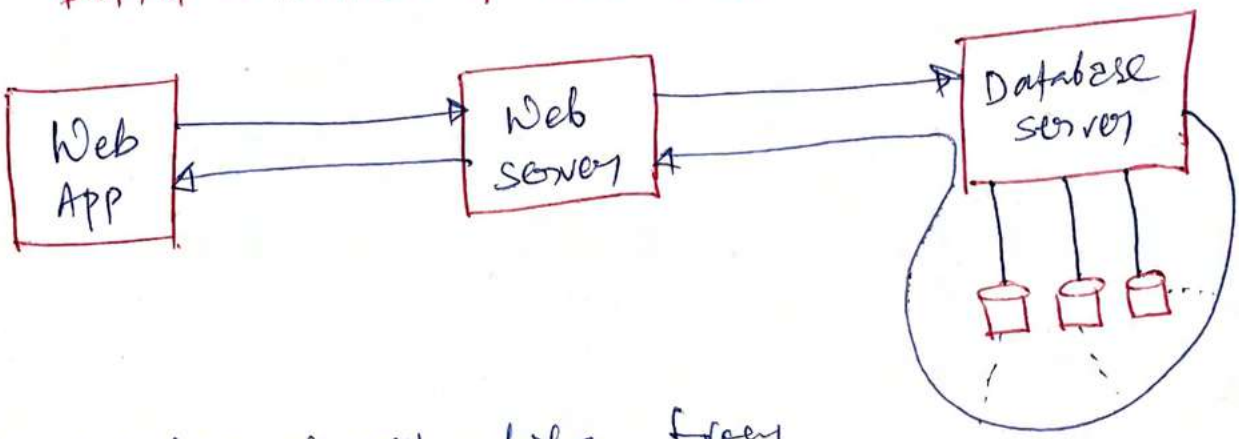
No damage : No need to protect C+A but still a little bit Integrity.



SECURE EMAIL EXAMPLE WITH SECURITY CONTROLS / MEASURES



DATA STATES W/ EXAMPLE

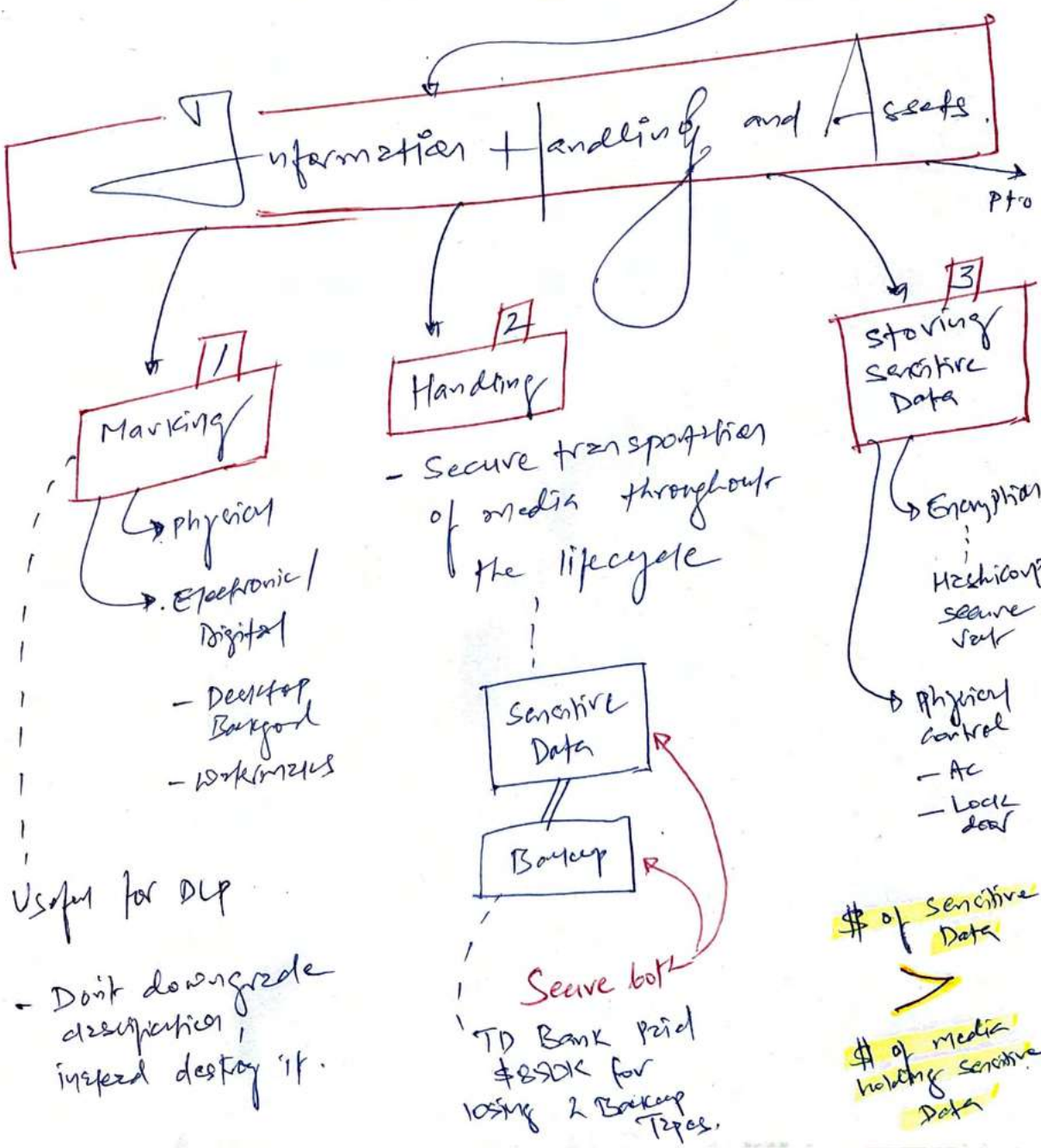


1. Web App request data from web server
2. Web server request data from Database server
3. DB server retrieves encrypted data from Database, convert to (decrypt) format so web App can understand.
   → Data At Rest (AES 256)
4. DB server again encrypt the data & send to web server
   → Data In Transit (TLS 1.2)
5. Web Server decrypt the data & send it to web App. It stores some temp data buffer while authorizing transaction & purge / delete data (from memory) when ~~web App~~ no longer requires.
   → Data In Use (TLS 1.2)

REGARDLESS OF SECURITY CONTROLS

DATA BREACH happens --

To prevent data breach, we need to manage sensitive data



4

Destroying sensitive Data

- High classified Data = complete Destruction
- lower classified Data = overwrite.

It's not just about destroying data, it's how we destroy it. Method matters.

5

Eliminating Data Remanence

Remance

(Ex girlfriend's memory trace)

Traces of Data Residue even after deleting it.

destroying data methods

- Erasing
  - Not secure
- Purging
  - clearing process multiple times
  - Not ideal for Top Secret data
- clearing / overwriting
  - Phase 1 1010
  - Phase 2 0101
  - Phase 3 1101 (replace random digits :)
- Degaussing
  - works for magnetic types + harddisks
  - Not for CD / DVD / SSD.
- Encryption
- Destruction
  - Physical destruction = most secure
  - Burning
  - SAD = disposing body.

ASSET / MEDIA

× → Decrassify + Purge
= $$$$

→ Destroy & buy new media
= less $$$

Data Retention — P.t.O for bigger picture

- What to retain?
- For how long?
- Where it will be retained?

AUDIT LOGS

Retention Period Expires = Destroy the data

--- Boeing paid $92.5 mil for 14,000 Email decrease types.

How can we protect Data?

!--- more in Domain 3

Data Protection Methods

- Symmetric encryption
  - AES
  - 3DES
  - Blowfish
- Transport encryption (TLS 1.2)
  - Remote VPN
  - IPSec
  - SFTP, SCP

Ownership

Who owns the DATA?

Who owns the asset?

1 DATA OWNERS ... NIST SP 800-18

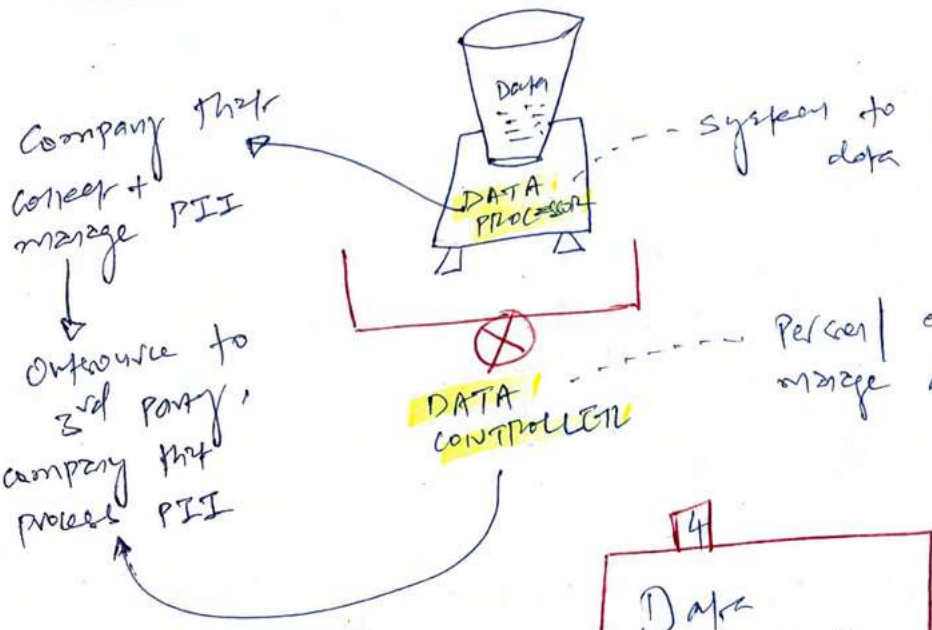
same person

2 ASSET OWNERS

↳ Data + Asset are classified + labled

↳ Appropriate security controls are implemented

3 Business Mission owners ---- own business process



4 Data Processors

European Commission + US Government / Department of Commerce ⟹ SAFE HARBOR PROGRAM

7 Privacy Shield Principles

→ organization can self-certify using these principles.

↳ (1) Notice :- From organization To customers on what info they collect & why they collect

↳ (2) Choice :- To opt-out / unsubscribe kind of.

↳ (3) Accountability for onward transfer :-

organization = comply (1) Notice & (2) Choice

↓

Forward / transfer info to 3rd party

↳ (4) Security : of Personal Data

↳ (5) Data Integrity & Purpose Limitation : only collect info as what's needed

↳ (6) Access : Individual to correct, amend, delete their PII

↳ (7) Recourse, Enforcement & Liability :- Mechanism to handle individuals complaints.

5

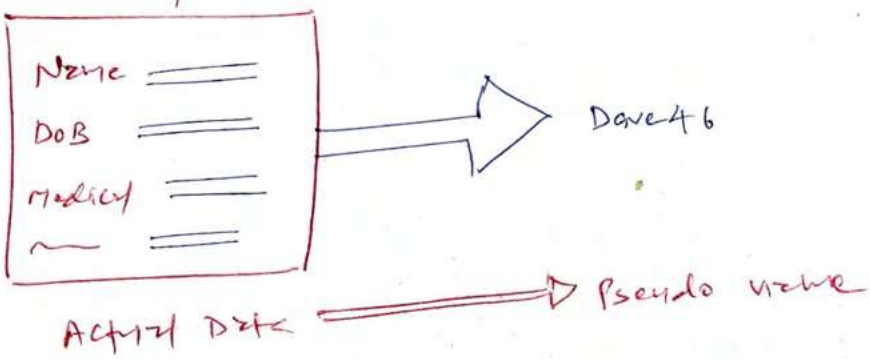
Pseudonymization

--- similar to Tokenisation

- GDPR context = Replacing data with Artificial Identifiers.

Sensitive Information Protection

- Encryption
- Pseudonymization.

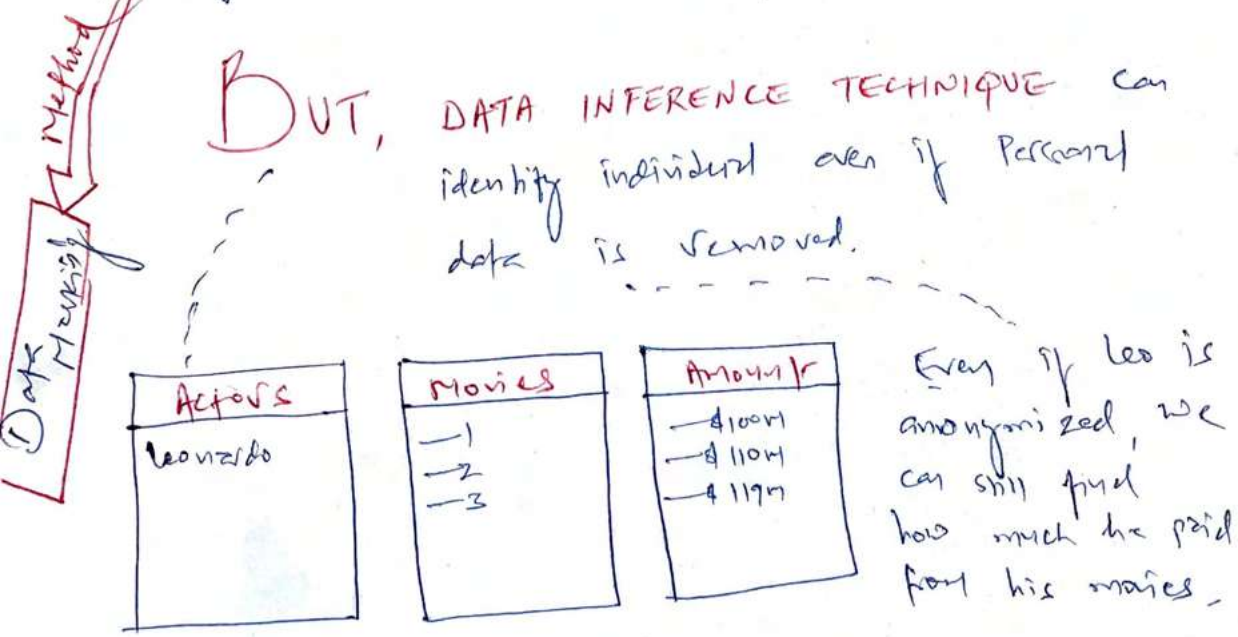


6

Anonymization

--- Removing all relevant data so it's impossible to identify the original data/ subject/ Person.

BUT, DATA INFERENCE TECHNIQUE can identify individual even if Personal data is removed.



Even if Leo is anonymized, we can still find how much he paid from his movies.

Data Masking vs Pseudonymization / Tokenisation

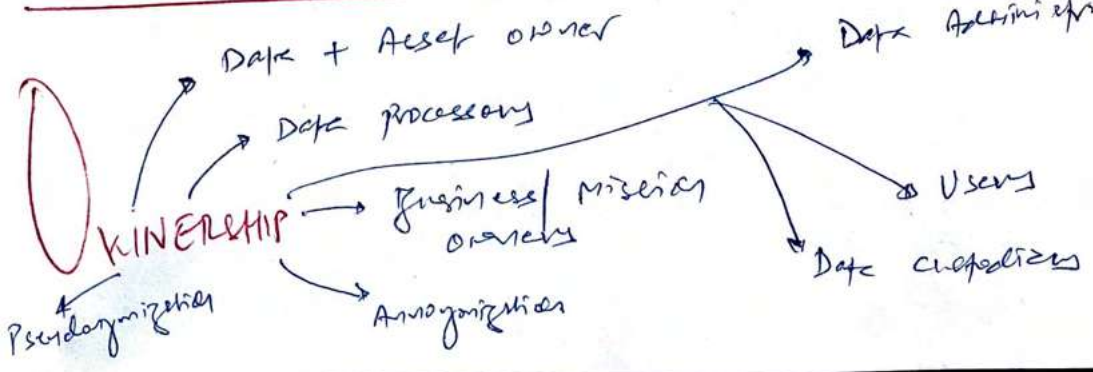
→ once masked, it cannot return to original state.

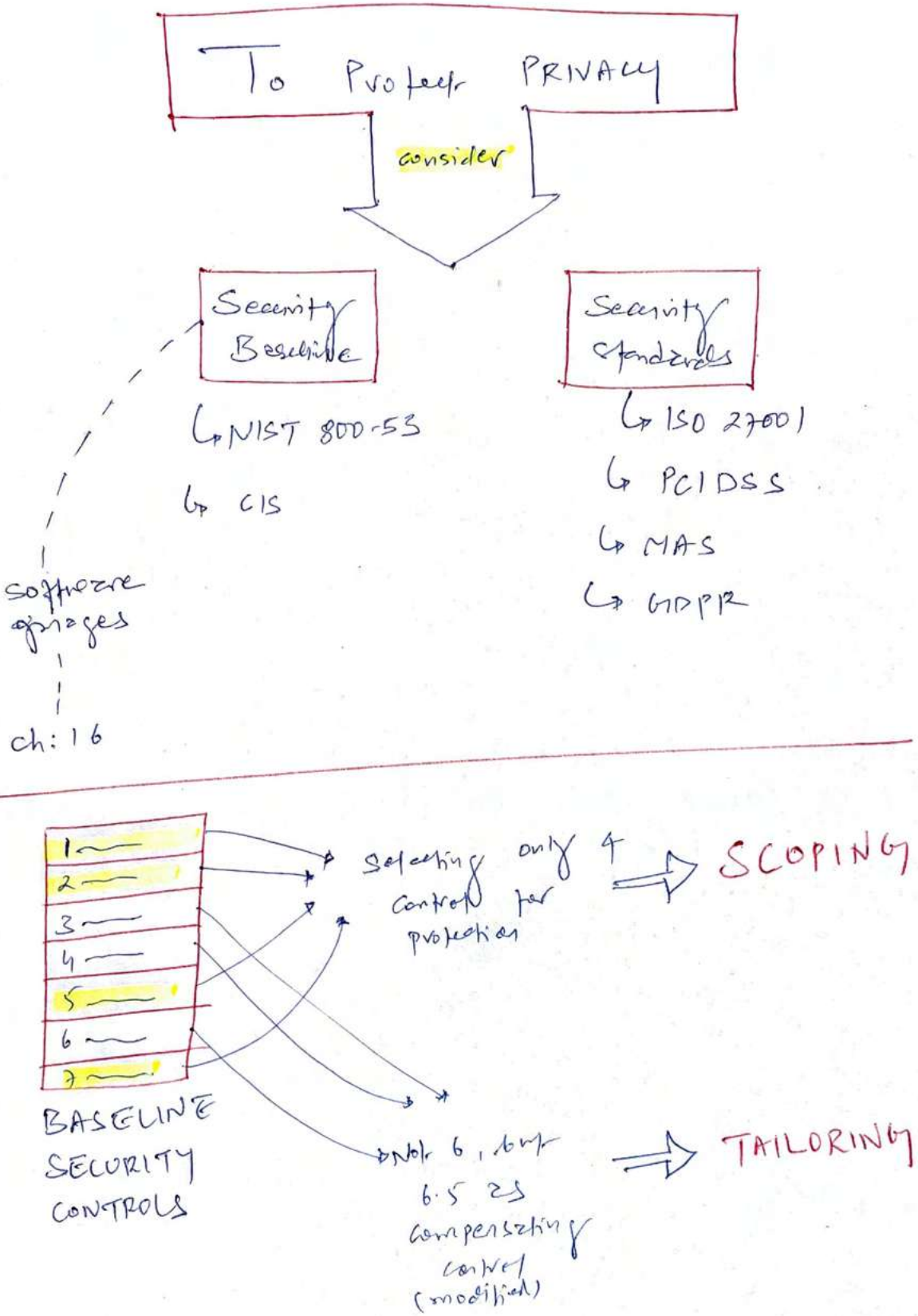
7 DATA Administrator ----→ Assign permissions based on RBAC / least privilege

8 DATA Custodians ----→ Data owner delegate day to day task to custodians

- maintains integrity and security of data
- Data is backed up.
- Data logs maintenance for Audits.

9 Users ----→ Have access to data they only need




To Protect PRIVACY
consider
Security Baseline
↳ NIST 800-53
↳ CIS
Security Standards
↳ ISO 27001
↳ PCIDSS
↳ MAS
↳ GDPR
software images
ch: 16
1
2
3
4
5
6
7
BASELINE SECURITY CONTROLS
Selecting only 4 control for protection
SCOPING
Not 6, but 6.5 as compensating control (modified)
TAILORING

★ Inventories

① Tracking Hardware

Problem : Pirated hardware / stolen or tampered hardware

Solutions — ISO 28000 : 2007
- secure supply chain
- Trusted source
- Trusted transportation network
- effective inspection process

② Tracking Software

Problems
- distribution of unlicensed s/w in company
- unlicensed s/w without patch = Hole in security
- Pirated software with backdoor entry : trojan

Solutions

Solution of software tracking problem = MULTIFACETED

- Application whitelisting
- Using Gold Masters - standard image for authorised software
- Enforce POLP - Not everybody should install s/w.
- Authorized scanning - periodic vul. scan.
- Device management Software - Unified Endpoint mgmt (UEM)

DATA RETENTION

what data to retain?

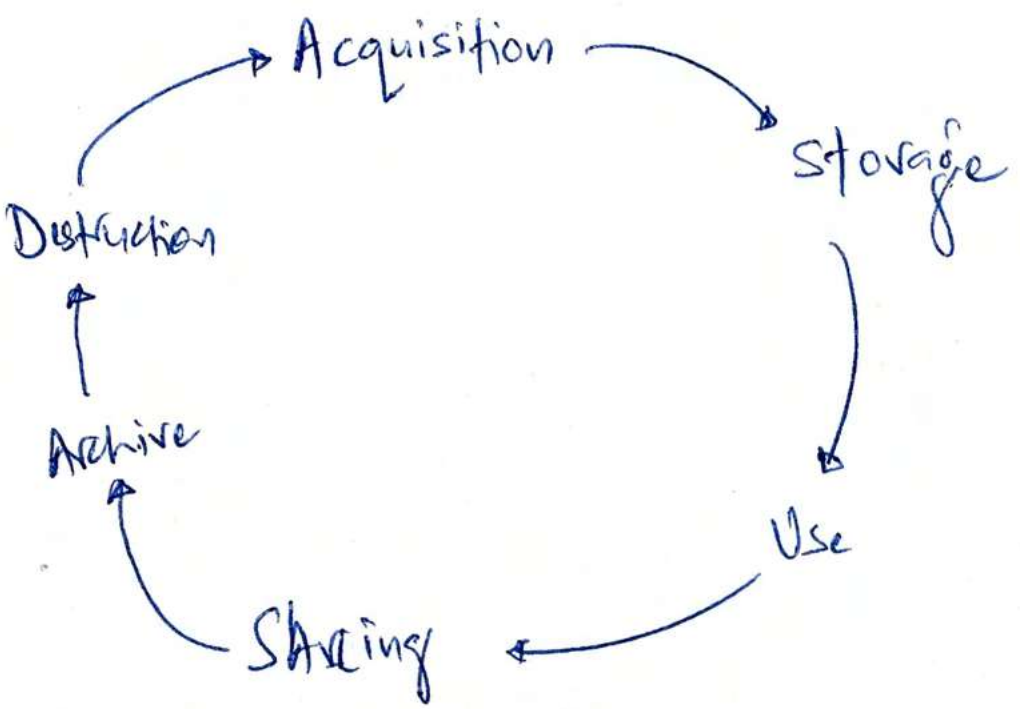
Where to retain Data?

How we Retain Data?

To ensure data is available in timely manner, consider four issues:

1. **Taxonomy**
   - Based on various categories
   - 2020, HR, IT, Marketing
2. **Classification**
   - Search data based on sensitivity
3. **Normalization**
   - Tagging scheme that make data searchable
4. **Indexing**

INFORMATION / DATA LIFE CYCLE



Note - Introducing Cryptography can add value to data life cycle

↳ USE = hashing for integrity

↳ ARCHIVE + DESTROY = Encryption for confidentiality.

6. CRYPTOGRAPHY & SYMMETRIC KEY ALGORITHMS

CRYPTOGRAPHY GOALS (P.T.O.)

- Confidentiality
- Authentication
- Nonrepudiation
- Integrity

Of sensitive information AT rest, in transit, in use

HISTORY

Caesar cipher

A → D
B → E
} ROT3

↳ Vulnerable to frequency analysis attack

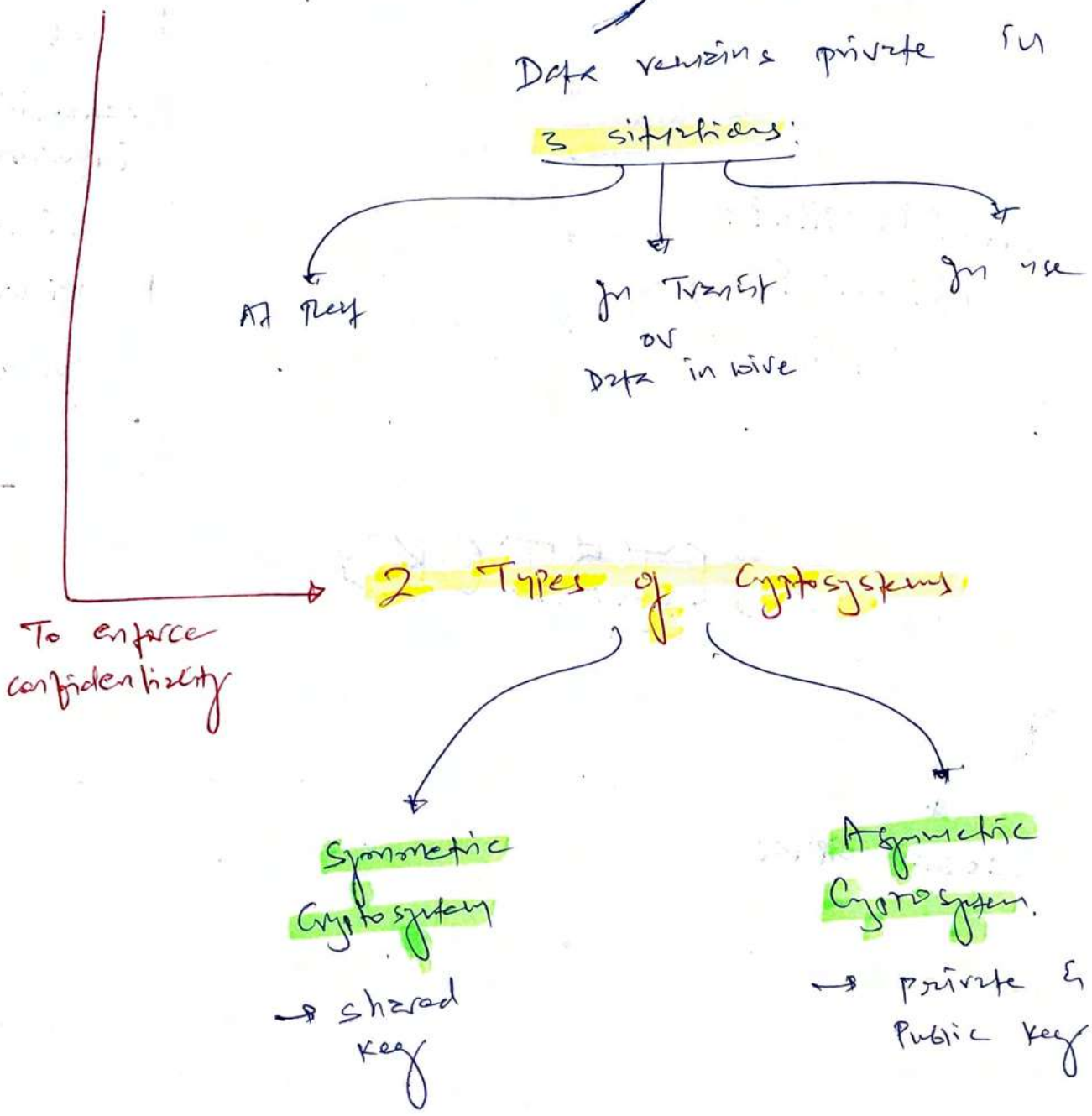
Note

↳ If you can decode using Frequency Analysis, then it's transposition cipher.

↳ Substitution cipher are more prone to Periodic Analysis

Examination of frequency based on repeated use of key

1. Confidentiality —— what it means?



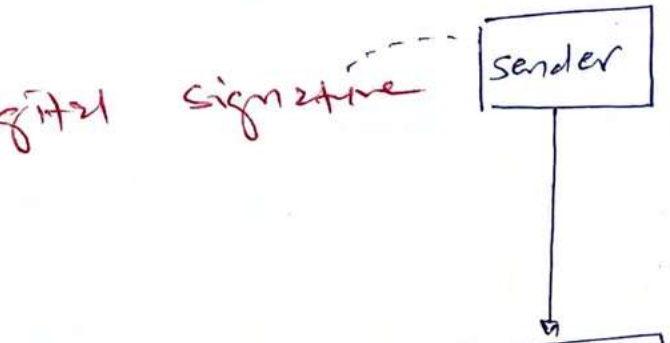
Think different kinds of Data with Attacks.

- Data At Rest — theft or loss of physical device
- Data in Transit — Eavesdropping
- Data in use — Unauthorized Access

2. Integrity —— what it means?

Data is not altered from the time it was created and the time it was accessed.

To enforce integrity → Digital signature

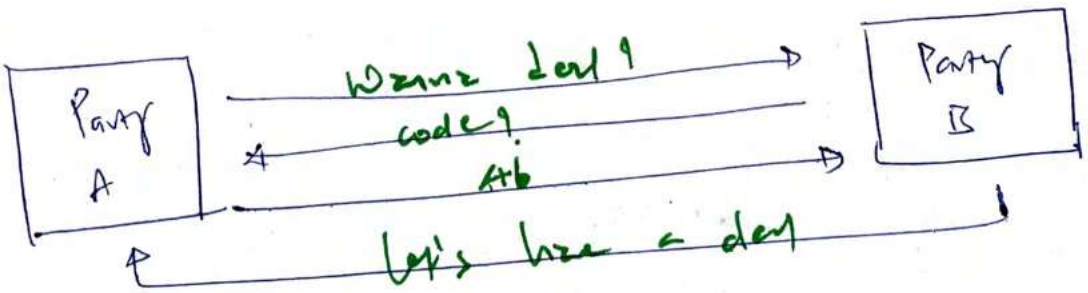


Validate digital signature

→ Ensures message wasn't altered in transit

3. Authentication —— what it means?

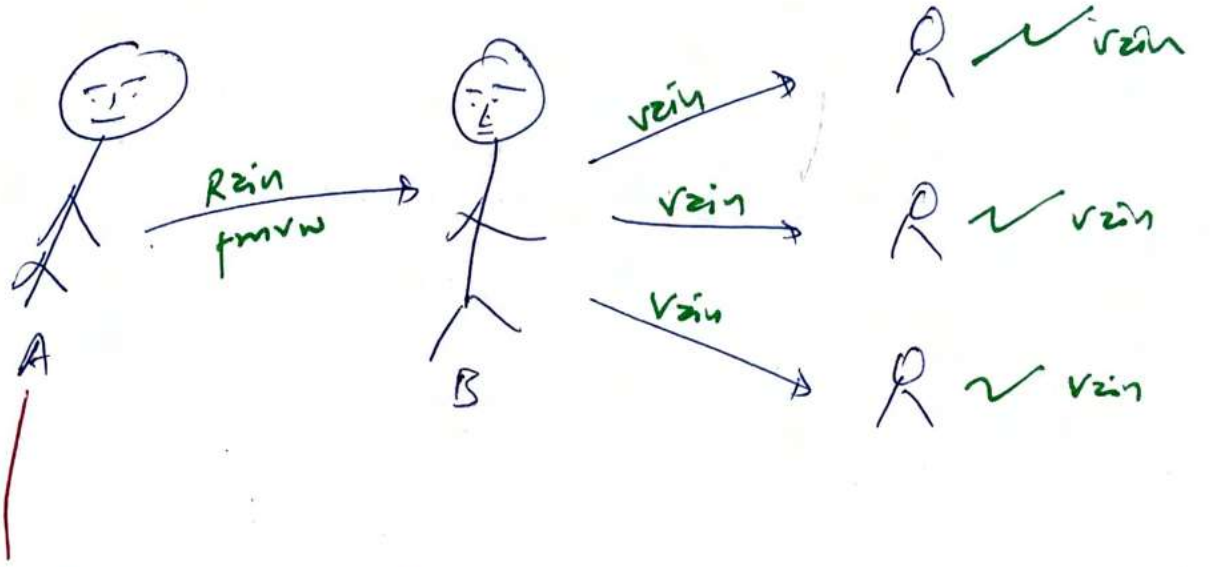
To make sure person is genine what he meant to be



→ Both party have a secret code to establish secure comm

→ Uses challenge-response authentication technique.

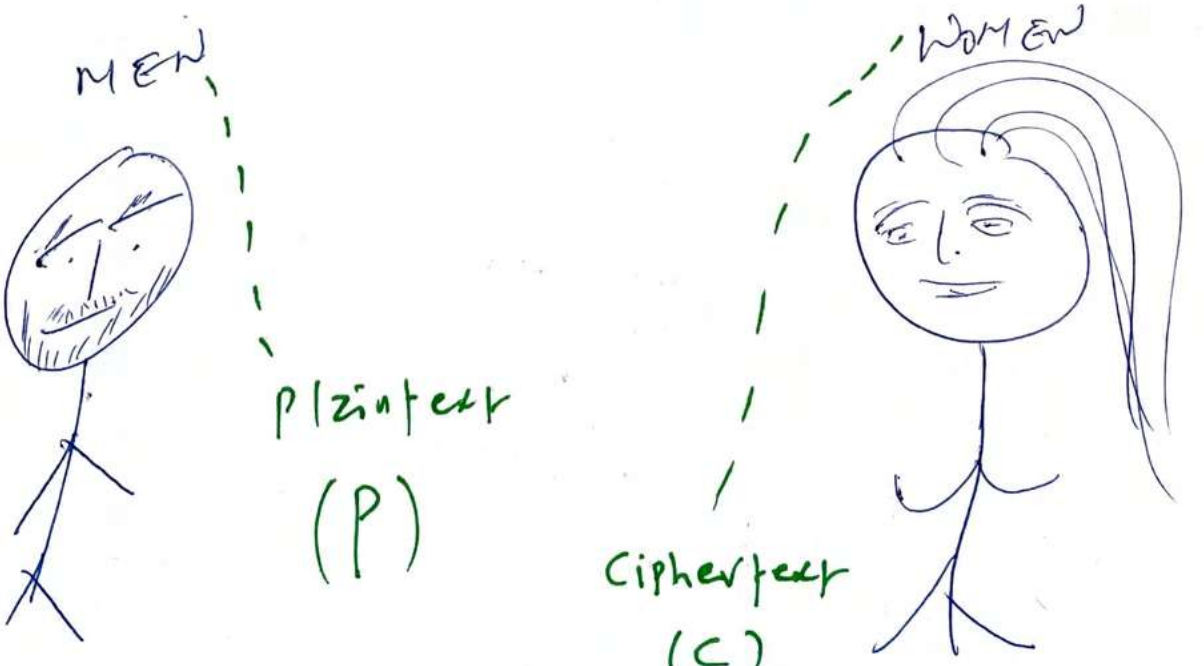
4. Nonrepudiation



Hey! But I didn't tell that.

↳ Symmetric key ≠ Non repudiation (Authenticity)

↳ Asymmetric key = Non repudiation



Cryptographic Algorithms $\propto$ KEYS = To maintain SECURITY

Secret Key

Private

Open to Public except crypto keys

= The Enemy Knows the system. (Kerckhoff's Principle)

CRYPTOGRAPHY CONCEPTS

X	Y	X ⊕ Y
0	0	0
0	1	1
1	0	1
1	1	0

EX OR

X	Y	X ^ Y
0	0	0
0	1	0
1	0	0
1	1	1

AND

X	Y	X v Y
0	0	0
0	1	1
1	0	1
1	1	1

OR

X	¬X
0	1
1	0

NOT

Modulo Function

8 mod 2 = 0

15 mod 3 = 0

10 mod 3 = 1

33 mod 8 = 1

6 mod 8 = 2

6 mod 8 =

One-way Functions

- Produce large prime numbers as output so finding input value becomes IMPOSSIBLE!

Nonce

(number used only once)

- Example of Nonce is IV - initialization vector
- IV is random string XORed with message

CORE IV concept

Salt

If IV is not used then two identical plaintext that are encrypted with same key will create same cipher text. Algorithm use IV & key to provide randomness in Encryption process.

- IV creates unique cipher text everytime message is encrypted using same key.

Zero-Knowledge Proof

↗ Prove knowledge to 3rd party without revealing secret / fear

Split Knowledge

↳ M of N control (M<=N)

Seperation of Duties

↳ E.g Key Escrow Database

Work Function

An estimation how long attacker will take to break a cryptosystem (work factor)

P.T.O End

Strength of Crypto system	=	cost & time of work function

$100K worth of data

~~Brute force~~

$105K worth of cryptography solution

remember ... Work function > Asset value

CRYPTOGRAPHY CONCEPTS (contd ...) → CIPHER

↳ Meant to hide true meaning of message

Don't confuse with

CODE

↳ Not all codes are secret

↳ "Eagle has landed" to report arrival of Enemy crypt

This can convey confidential message but may not achieve confidentiality

difference:

↳ Achieves confidentiality with variety of techniques.

↳ codes work on words and phrases while ciphers works on individual characters and bits.

1. Transposition cipher - scramble

↳ scrambling / rearranging letters of plaintext ⇒ ciphertext

↳ can use "columnar transpotion" for more complexity

Block cipher

2. Substitution Cipher

↳ Recall caesar cipher (ROT3)

↳ Uses encryption algorithm to replace characters of plaintext with other characters.

↳ Polyalphabetic : Another substitution cipher

- Protects against direct frequency analysis but vulnerable to Periodic analysis.

3. One-time Pads — The only perfect Cryptosystem

↳ aka Vernam cipher

↳ The key length is as long as message!

↳ impossible to break when used correctly

- need physical protection
- one time pads must be randomly generated values
- one pad = one time use
- long keys = difficult to distribute
- Securely distributed to its destination

VENONA

Entire soviet union project was declassified as one-time pad ~~didn't~~ generated receiving Key instead of random one.

4. Running Key cipher

↳ Book cipher ——— MOBY DICK
↳ page 46
↳ 3rd para

↳ Unlike one time pad which requires physical exchange of pads, two parties need a common book.

p.t.o End 10,000 ft.

2 types of symmetric Algorithms
- Block cipher
- Stream cipher

5. Block Cipher

↳ Transposition as example of block cipher + many modern encryption algorithm.

6. Stream Ciphers

↳ one character at a time — ceesar / one time pad

↳ Even Block cipher but buffer fills all data & process one at a time

---

Cryptographic algorithm's 2 basic operation to obscure plaintext message

Confusion — Attackers can't determine plaintext
- Attacker can't determine relationship b/w ciphertext & plaintext

Changing ciphertext selecting ciphertext to determine key.

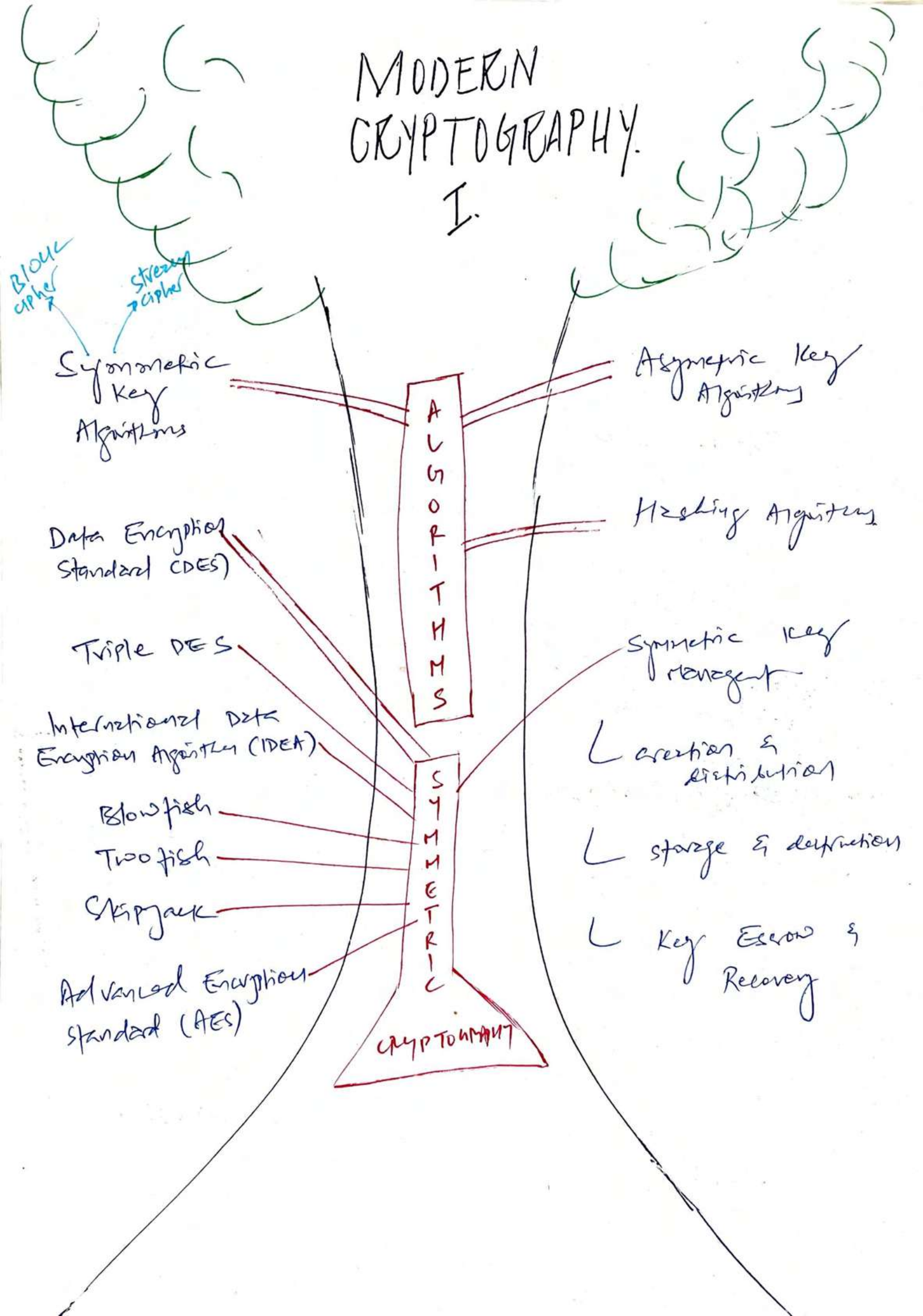
p.t.o End

better clarity

Diffusion
- change in plaintext results in multiple changes throughout the ciphertext

MODERN CRYPTOGRAPHY.

I.



Cryptography perspective

THEN

Algorithm + secret key

↑ Hide from public

"Security through obscurity"

NOW

Algorithm

Secret keys — secret

Available to public = improves security

Cryptographic keys

the length of the key directly relates to work function of the cryptosystem.

longer = secure

3 types of Algorithms

- Symmetric Encryption
- Asymmetric Encryption
- Hashing

1. Symmetric key Algorithm.

↳ private key Cryptography

- Not to confused with private - public key pair.
- Private key means two people share same secret (to encrypt & decrypt message).

↳ Problem with Symmetric Key Cryptography

- * No non-repudiation but provides Confidentiality
- Key distribution = problem → QKD: one of quantum Key Distribution will solve this problem
- Not scalable
- Frequent Key generation

HOW MANY KEYS?

$\frac{100\ (99)}{2} = \frac{9900}{2} = 4950$

$\frac{n(n-1)}{2}$

n = parties

Strength ..... Weakness

- It's free.

2. Asymmetric Key Algorithms ---- ch:7

best pair

- Sender Encrypt message with Receiver's public key
- Receiver Decrypt message with it's own private key.

- once sender encrypt, he/she/they can't decrypt it with their private key

HOW MANY KEYS?

↳ DOUBLE IT

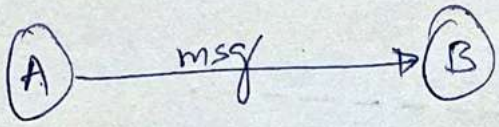
2 → 4
5 → 10
10 → 20
100 → 200

What's happen when we browse website (OSCP PART)

- Browser gets website server's Public Key, browser generates Symmetric Key & encrypt with website server's public key

- Web server decrypt with it's private key

↳ Asymmetric key algorithm = support for Digital Signature



How B verify that msg came from A?

1. A ~~Creates~~ creates message digest with hashing algorithm
2. A Encrypt msg with own private key
3. B decrypt msg with A's public key.

↳ Asymmetric strengths

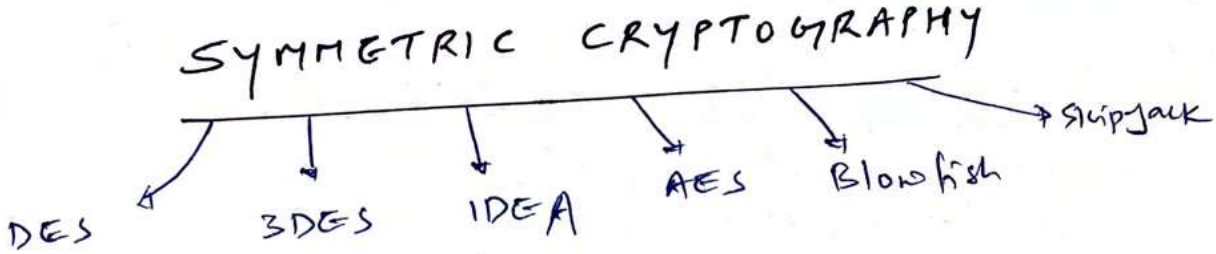
- Every new user = one pair of public-private key
- Generate only key if Private key is compromised
- Easy key revocation / removing user from system
* - Provides nonrepudiation, integrity & confidentiality, authentication
- Easy key distribution process = make your public key available on internet.
* - No preexisting communication link needs to exist = Batman vs Joker can be friends
* - scalable

↳ Asymmetric weakness = slow

3. Hashing Algorithms --- Ch: 7

↳ Recall MESSAGE DIGEST as part of Digital signature support from Asymmetric Key Algorithms.

Hash algorithm produces MD.



* Data Encryption Standard (DES)

- Insecure, but still a building block of 3DES
- 64-bit block cipher for all five modes of operation techniques
- Uses 56-bit Key to drive encryption & Decryption process.

Remaining 8-bits are used for detecting tampering or corruption of the key.

→ all 64-bit block

5 modes for DES operation:

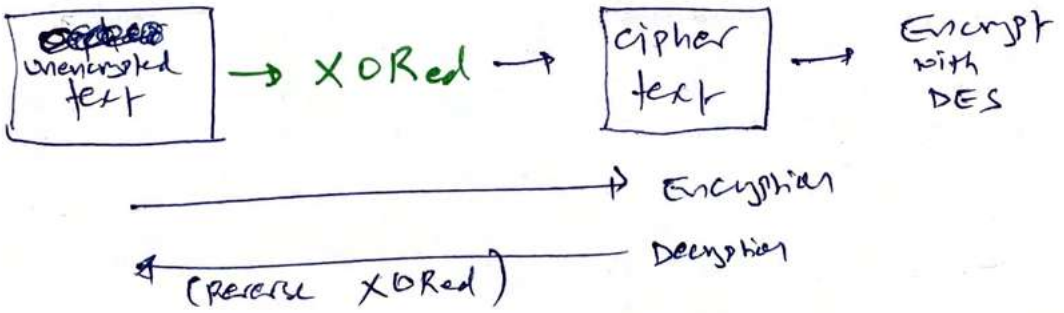
i) ECB - Electronic code Book

- Encrypts the block with chosen key. If algorithm encounters same block, it produces same encrypted block.

Using same key + lock for all the doors → least secure

- Used to exchange small amount of data.

ii) CBC - Cipher Block chaining



- Implements IV & XOR: produces unique output everytime operation is performed

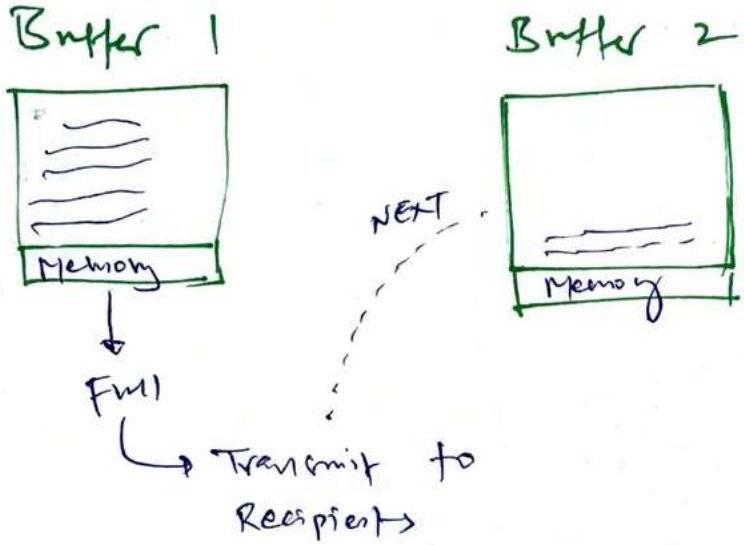
* If block is corrupted during transmission, it's impossible to decrypt that block & following blocks.

chaining

Output Feedback Mode solves this problem

iii) Cipher Feedback - CFB

- Stream version of CBC, uses XOR
- Instead of blocks, it uses memory buffers
- It uses IV and chaining.



iv) Output feedback - OFB

- Similar to CFB, instead of XORing encrypted version of previous block of cipher text, DES XORs plaintext with seed value

* Advantage: No chain vertical like transmission error in CBC

v) Counter Mode - CTR

- ideal for parallel computing as it allows encryption & decryption into multiple independent steps.
- Use stream cipher similar to CFB. Instead of creating seed value for Enc/Dec. operation, it simply use counter increments for each operation.

* Triple DES (3DES)

- Because DES' 56-bit key length was insecure.

4 versions

1 DES-EEE3

Plaintext × three-times Encryption with different keys

K1 K2 K3

$E(P, K)$ — Encryption; P: Plaintext; K: key

$$E(K1, E(K2, E(K3, P)))$$

Effective key lc = 168 bits

After Attack KL = 112 bits.

2 DES-EDE3

- Same as **1** but replace second encryption operation with decryption

$$E(K1, D(K2, E(K3, P)))$$

KL = 112-bits

3 DES-EEE2

4 DES-EDE2

(only uses two keys)

Effective KL = 112-bit

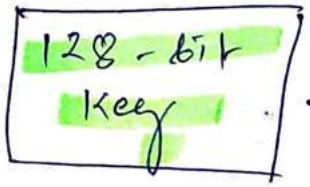
After Attack KL = 80-bit

$$E(K1, D(K2, E(K1, P)))$$

$$E(K1, E(K2, E(K1, P)))$$

* International Data Encryption Algorithm (IDEA)

- Developed to respond insufficient KL in DES
- Like DES, it uses 64-bit cipher block of plaintext / ciphertext
- Unlik DES' 56-bit KL, IDEA use 128-bit KL.
- IDEA capable of using all 5 modes of DES operation



— broken up into a series of operation into 52 16-bit subkeys

- IDEA implementation: Pretty Good privacy (PGP) for secure email package.

* Blowfish —more secure→ Twofish

- Bruce Schneie's alternative to DES & IDES
- 64-bit block } fast
- KL range: 32-bit to 448-bit

- 128-bit block
- KL: 256-bit
- 2 techniques
  - Pre-whitening
  - Post-whitening

* Skipjack

- 64-bit block & key
- KL: 80-bit
- Supports DES's 5 operation modes
- Embraced by US Government

Not embraced by cryptographic community due to mistrust of Escrow procedures within US Government.

TWIST

[Supports ESCROW of Encryption keys.

* RC5 (River cipher)

- From People who developed RSA Asymmetric Algorithm
- Block size: 32, 64 or 128 bits
- KL: 0 to 2048 bits

* AES - Advanced Encyption standard

- 2000: Nist announced AES / Rijndael
- KL: 128-bits, 192-bits, 256-bits
  - 128-bits: 10 rounds of Encryption
  - 192-bits: 12 rounds
  - 256-bits: 14 rounds
- Only allows 128-bit blocks

* Skipjack

- 64-bit block of text
- KL : 80-bit
- Supports DES's operation modes
- Embraced by US Government

TWIST

Not embraced by cryptographic community due to mistrust of Escrow procedures within US Government.

Supports ESCROW of Encryption keys.

* RC5 (River cipher)

- From People who developed RSA Asymmetric Algorithm
- Block size : 32, 64 or 128 bits
- KL : 0 to 2048 bits

* AES - Advanced Encryption standard

- 2000 : Nist announced AES / Rijndael
- KL : 128-bits, 192-bits, 256-bits
  - 128-bits : 10 rounds of Encryption
  - 192-bits : 12 rounds
  - 256-bits : 14 rounds
- Only allows 128-bit blocks

याद रखने - Symmetric Memorization chart

Name	Block size	Key size
Data Encrypt. Standard (DES)	64-bit block cipher	56 bits
3DES	64	112 or 168
IDEA (used in PGP) - uses DES's 5 modes	64	128
Blowfish — uses variable key strength	64	32-448
Twofish (Pre-whitening, Post whitening)	128	1-256
AES	128	128, 192, 256 (10) (12) (14)
Skipjack	64	80
Rijndael	variable	128, 192, 168
Rivest cipher 2 (RC2)	64	128
Rivest cipher 5 (RC5)	32, 64, 128	~~0 - 2040~~ 0 - 2040

SYMMETRIC KEY MANAGEMENT

Creation & Distribution of symmetric key

- Diffie-Hellman - Page 227
- Public Key Encryption
  - IPSec
- Out-of-band method
- offline Distribution
  - ♥ love letter in her hand

Secure-RPC (S-RPC) employs Diffie-Hellman for key exchange.

Storage & Destruction of sym. keys

- Vault
- Principle of Split Knowledge
- Consider Key rotation
- Never store Encryption key where Encrypted Data resides

Key Escrow & Recovery

- When Government wanted to obtain cryptographic key under court order

2 APPROACHES

Escrowed Encryption Standard

- idea behind Skipjack
- technology is available but likely to happen where Government can decrypt the ciphertext.

Fair Cryptosystem

- Secret key divided into 2 or more pieces & given to independent 3rd parties

To Enforce confidentiality

Symmetric → shared key

Asymmetric → Private | public key

To Enforce Integrity

Digital signature

To Enforce Authentication

challenge-response technique

To Enforce Nonrepudiation

Seperation of Duty

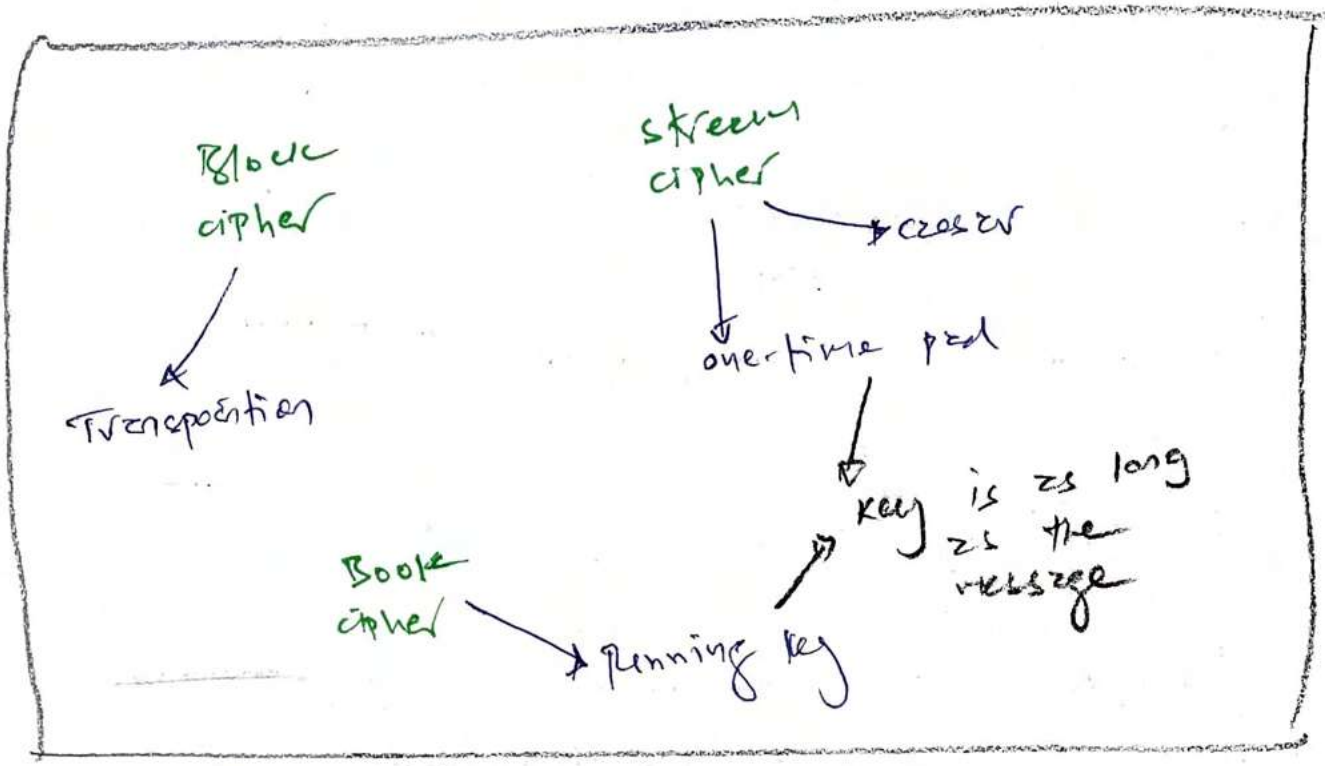
Split knowledge → M<=N → of key escrow database

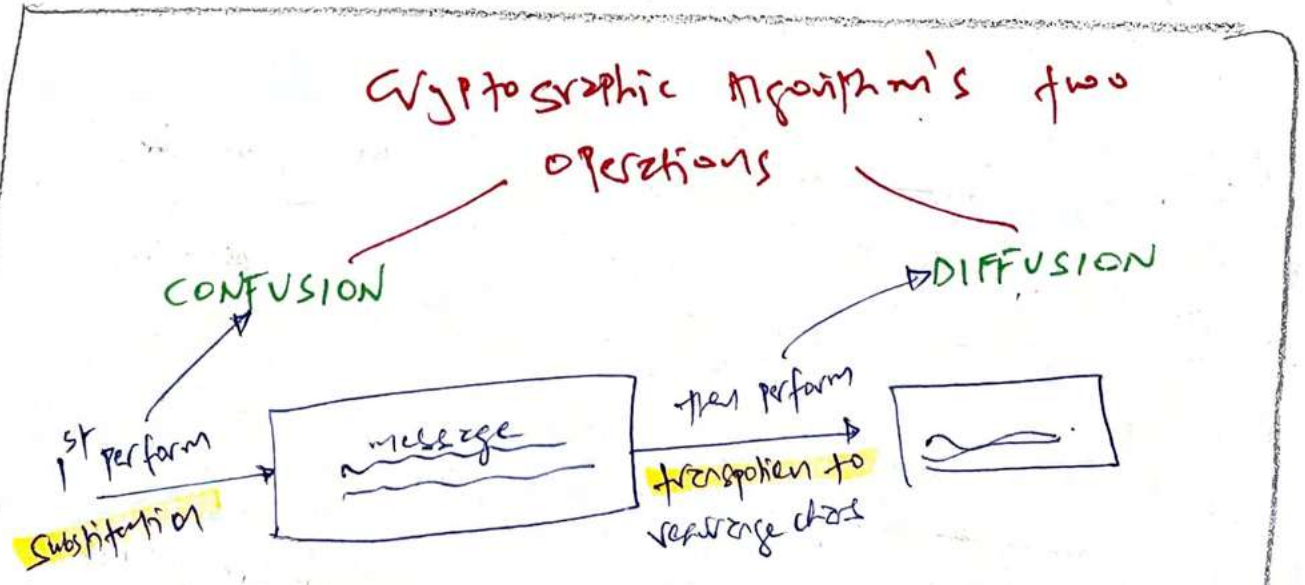
3 of 8 require to launch Nuclear attack

- min 3 person required out of 8
- 3(M) is less than N(8)

codes —— words & phrases

ciphers —— bits & characters





- confusion makes relationship b/w plaintext & keys complicated
- Diffusion → plaintext has influence over ciphertext. occurs when change in plaintext results multiple changes throughout in ciphertext.

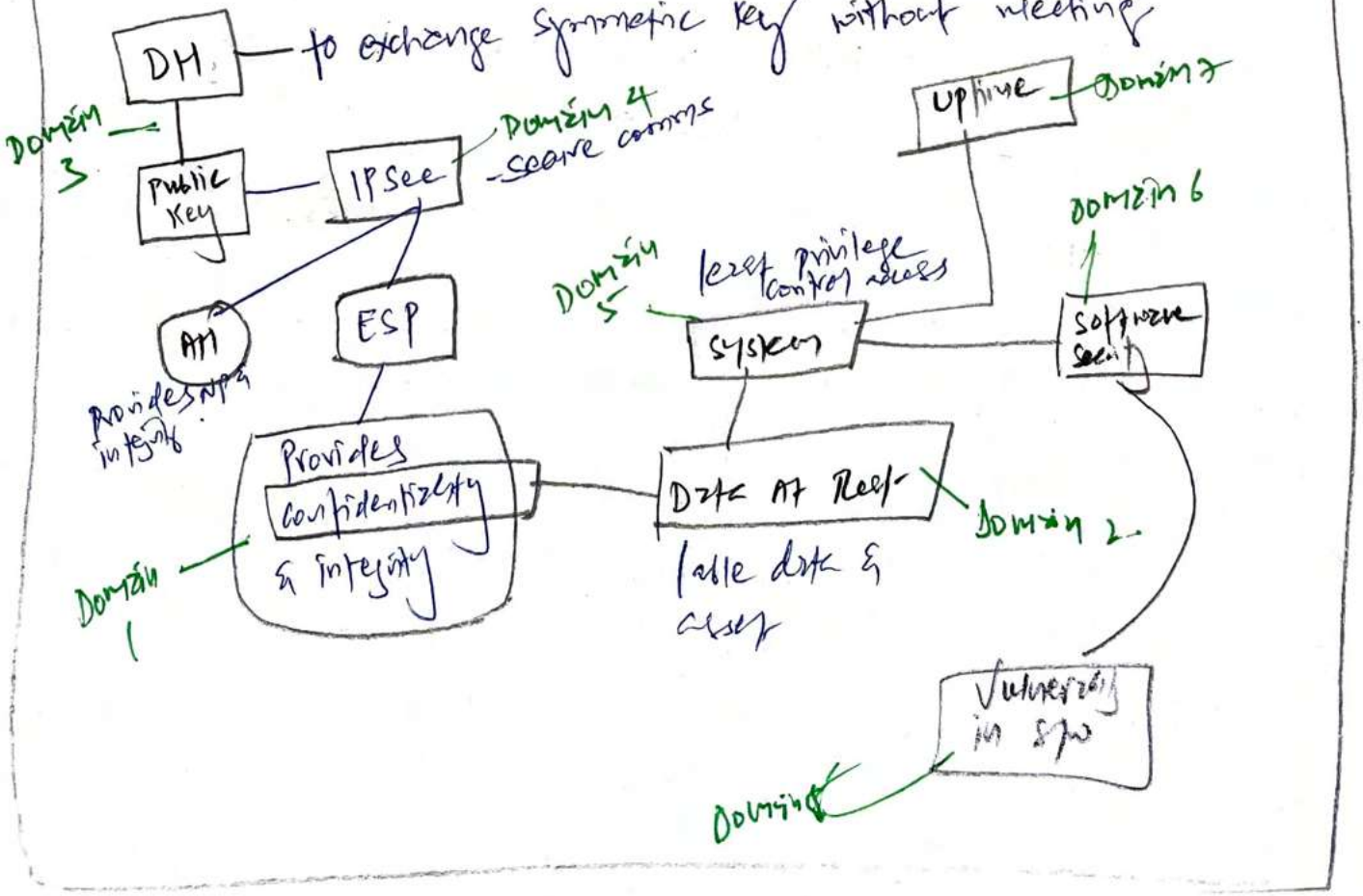
Symmetric → Confidentiality.

Asymmetric → Confidentiality, Nonrepudiation, Authentication, Integrity

Why Symmetric Encryption ≠ Nonrepudiation

Any communication party can Encrypt and decrypt message with shared key, there is no way to know where message is originated from.

Domain correlation example



SYMMETRIC KEY CRYPTOGRAPHY

- AES
- Blowfish, Twofish
- Skipjack
- IDEA
- DES + 3DES

Symmetric Algorithms

Block cipher

- 640 bits of message chopped into → 10 individuals block of 64-bits
- Strong cipher contains two attributes
  - Confusion – Substitution
  - Diffusion – Transposition
    - Related concept "Avalanche Effect"
    - A tiny input to Algorithm significantly chage the output

Stream cipher

- Individual bits of plaintext XORed to produce ciphertext ← Uses Keystream Generators

STREAM CIPHER

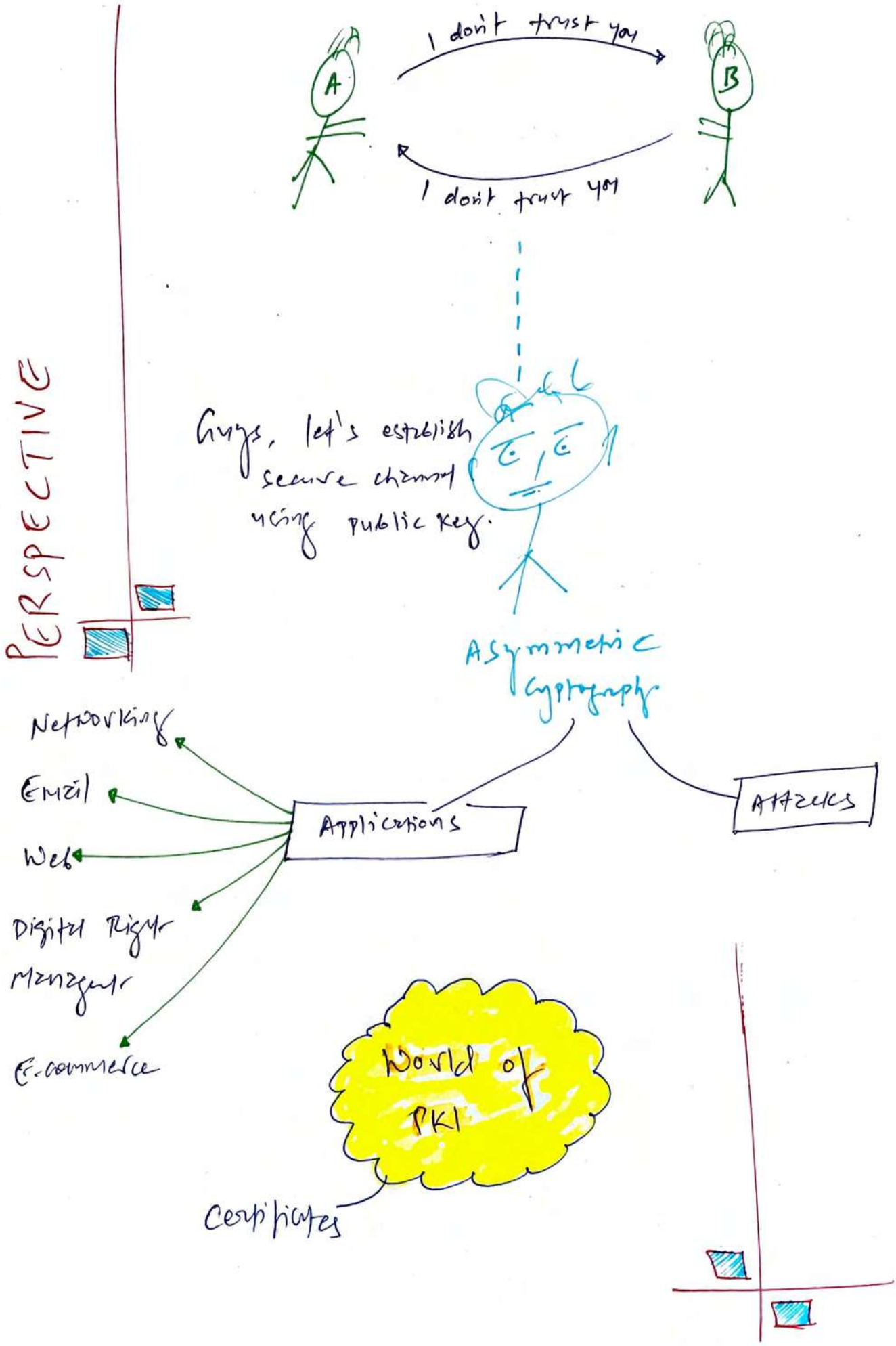
- Requires randomness (refer to IV concept)
- Require more processing power, so used at hardware level while Block cipher takes less processing power & suited at software level.

Symmetric Key Cryptography

e.g.

- Secret key Cryptography
- Session key Cryptography
- Shared key Cryptography
- Private key Cryptography

7. PKI & CRYPTOGRAPHIC APPLICATIONS



ASYMMETRIC CRYPTOGRAPHY

Three most common public key cryptography system used today:

1. Public & Private Keys
   - Public key freely available to anyone with whom they want to communicate.
     (BATMAN VS JOKER)
   - Beauty of public key cryptography

2. RSA
   - 1024 bits KL
   - has one-way function
   - Factors large prime numbers into their original prime numbers.

   jump:- RSA often used as key exchange protocol, means it can encrypt symmetric key for secure delivery to destination.
   (RSA often used with AES)

3. El Gamal

ELGAMALDOUBLE

Plaintext —Encryption→ Ciphertext
2048-bits 4096-bits

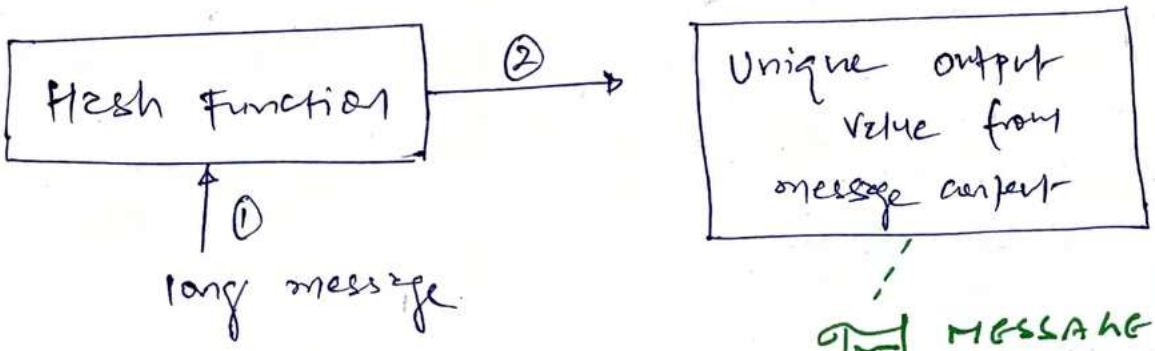
- it doubles the length of message it encrypts, data transmission becomes hard for narrow bandwidth circuits.

CRYPTOSYSTEM	KL
RSA	1024 bits
DSA	1024 bits
Elliptic curve	160 bits

- Equivalent

Any input
Fixed output → HASH FUNCTIONS ---- ONE-WAY
---- collision-free

cryptography system & Digital signature → Integrity



MESSAGE DIGEST (MD) 128-bit or larger

MD Generated by Sender & transmit to receiver with message for two versions.

Reeipient can use Same hash Function to recompute MD.
if values same = good.
If values are differt = message was tempered.

MD can be used to implement Digital Signature

INTEGRITY

NON REPUDIATION

* Four common hashing Algorithms :

SHA

- Secure Hash Algorithm

SHA-1

- takes an input of arbitrary any length & Produces 160-bit message digest.
- Process message in 512-bit blocks

SHA-2 : Four variants

a) SHA-256
- 256-bit MD
- 512-bit block size

b) SHA-224
- truncated version of SHA-256
- 224-bit MD
- 512-bit blocksize

c) SHA-512
- 512-bit MD
- 1024-bit blocksize

d) SHA-384
- 384-bit MD
- 1024-bit blocksize

HAVAL

- Hash of variable length
- Produce MD of 128, 160, 192, 224 & 256 bits

MD2

- 128-bit MD

MD4

- 128-bit MD
- 512-bit blocksize

MD5

- 128-bit
- HAVAL is MD5 variant

MD2 + MD4 + MD5 + SHA-1

NOT SECURE

SHA-2

Almost secure but has SHA-1 weaknesses.

SHA-3 SHA-384

∴ Federal Govt. approved Digital signature standard

DIGITAL SIGNATURES

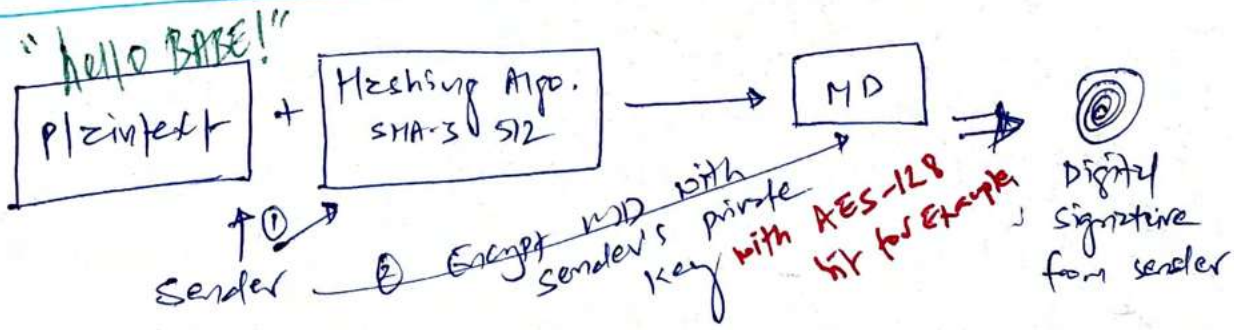
one of the reason why message digest (MD) is created. To implement Digital signatures.

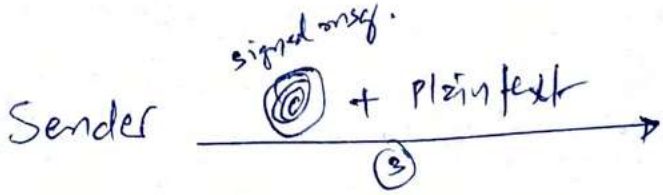
2 Goals

- To enforce Non-repudiation
- To maintain Integrity of the message

Digital signature Algorithm = 1. Public key Cryptography & 2. Hashing Functions

Process (Refer to remarkable notes)





④ Decrypt msg with sender's public key

Receiver also creates MD with same hashing function & plaintext ⑤

⑥ Receiver compare his MD with sender's MD — Match! / Don't match.

digital signature → yes
Integrity, Authentication, Nonrepudiation

↓ NO
Confidentiality

Trivia :- What can sender do / add extra step for message privacy / confidentiality ?

Ans: We can encrypt entire Digital Sig. process with Asymmetric Encryption

Need Partial Digital Signature ?

→ HMAC
(Hashed message authentication code)

Relies on shared secret key

⇓

[Symmetric key cryptography

✓ Integrity

✗ Nonrepudiation

Digital Signature Standard (DSS)

→ Acceptable for Federal Information processing Standard (FIPS) 186-4

→ MUST use SHA-3 Hashing Function

3 Approved standard Encryption Algorithms

→ Digital signature Algorithm (DSA) --- FIPS 186-4

→ RSA Algorithm ------ ANSI X9.31

→ Elliptic-curve DSA (ECDSA) --- ANSI X9.62

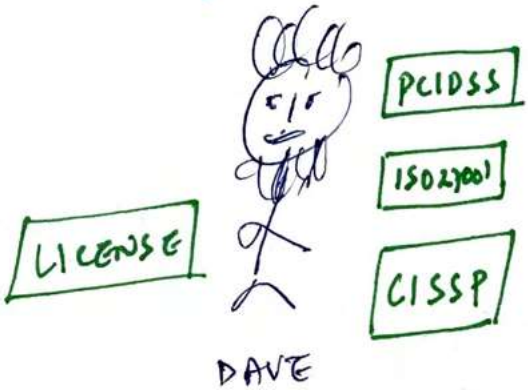
PUBLIC KEY INFRASTRUCTURE (PKI)

Nonrepudiation, Integrity, Authentication & Confidentiality: Provides

PKI = पंजीयन

To establish communication b/w two parties that are previously unknown to each other.

* certificates = Endorsed copy of Individual



All of these certificates are signed by respected Certificate Authority (CA)

(ISC)²

VICRoads

Godaddy

Digicert

They validate user identities & give heads-up to CAs to issue Digital certificates.

Registration Authorities

Assist

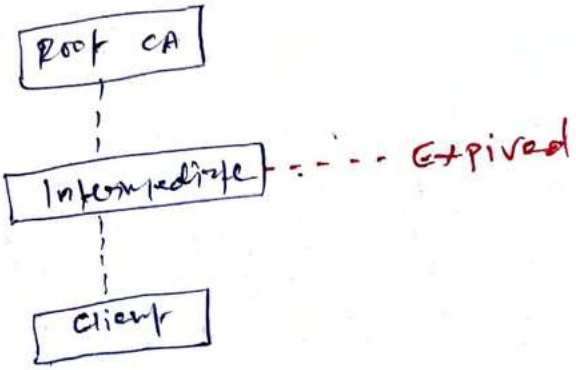
Certificate Authorities

--- vistaIndia

offload burden

---- Netflix

Certificate Path Validation (CPV)



* Certificate Generation & Destruction

nothing but a Public Key

Enrollment

① Prove your identity to CA / VicRoad

② Provide your public key to CA

③ CA creates X.509 digital certificate that contains your identity + Public key

④ CA signs (digitally) with CA's private key certificate

⑤ We can safely distribute with other parties / drive on the road.

we can decrypt with our public key (or) this could be CA's public key

Verification

* When we receive digital certificate from someone with whom we want to communicate

↳ check CA's digital signature using CA's public key

↳ check if certificate is revoked (CRL)

↳ OCSP

② Either we can provide our public key to CA or we can ask CA to provide public key + private key

Revocation

Certificate Revocation List (CRL)

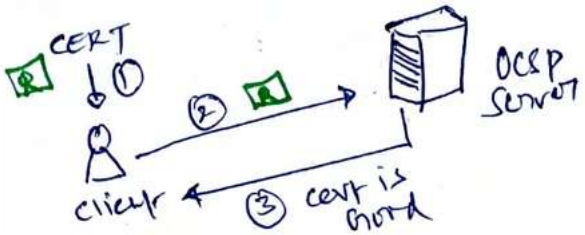
- Part of CA's inventory
- Most common method but huge latency.

Note - CRL contains serial number of Digital certificates, serial number must be part of CRL

CA must provide private key to verify if it is issued by same CA

Online Certificate Status Protocol (OCSP)

- Removes CRL's latency
- Real-time verification



ASYMMETRIC KEY MANAGEMENT

- Consider Key length
- Secure key in Vault
- Key Rotation
- Backup Key
- Retire Key after use
- Use Key Escrow Service

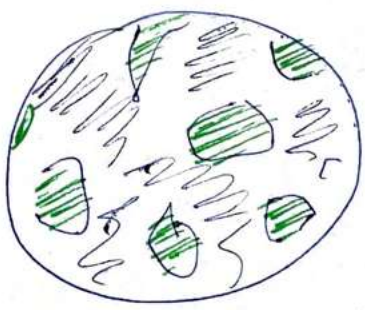
HSM — Hardware security modules

- Hardware devices to store & manage encryption keys

Cloud-based HSMs

YUBIKEY

APPLY CRYPTOGRAPHY



REAL WORLD APPLICATIONS

APPLIED CRYPTOGRAPHY

Data at rest

Portable devices

- Most OS = Encryption file system + smartphones
- Modern computers = TPM (Trusted platform modules)
  - Storage & management of keys used for Full Disk Encryption (FDE) solutions.

Data in transit

Email

Secure Email
- P.t.o End — PGP
- S/MIME (use of X.509)

If you want

Confidentiality → Encrypt the msg

Integrity → Hash the message

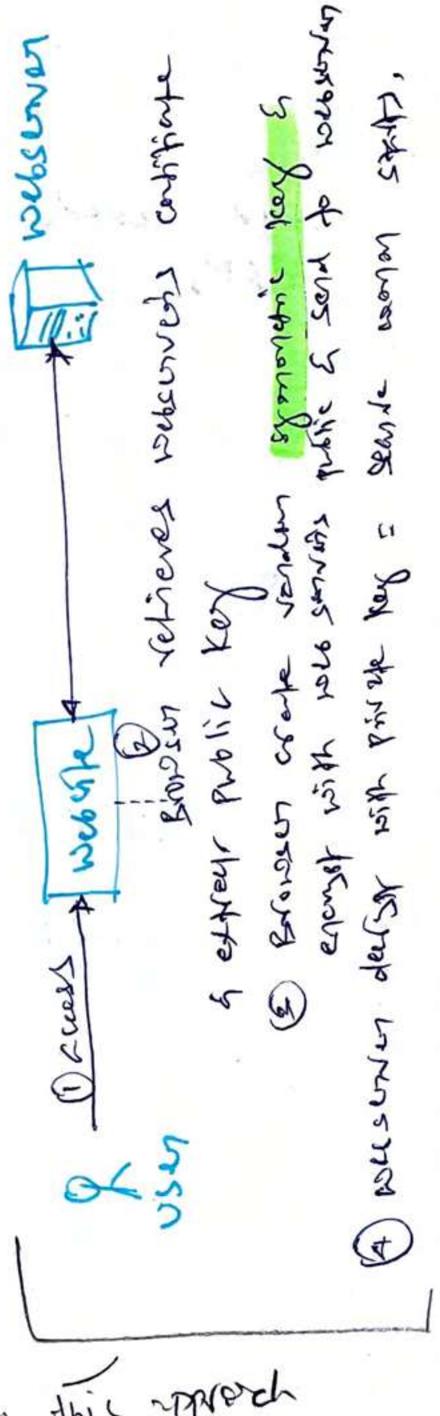
Authentication + Integrity + Non-repudiation + Confidentiality → Encrypt the msg + digital signature

Steganography & watermarking

isteg

Web Application

- SSL 3.0 → Poodle vulnerability
- TLS V1.2 — Replacement



why this approach is fascinating

LP10 End

DRM s/w uses ENCRYPTION to enforce copyright restriction on digital media.

DRM - Digital Rights Mgmt

music

movies

ebook

Video Game

Document

High Bandwidth Digital Content protection (HDCP)

- HDMI, DVI interface, display port

Advanced Access Content System (AACS)

- Blue-ray, DVD media

Adobe provides ADEPT - Adobe Digital Experience Protection Technology

- Uses AES for encryption & RSA for encryption to protect AES key.

Use encryption to protect docs/ sensitive info.

Networking

CIRCUIT ENCRYPTION

2 Encryption techniques to protect data while traveling over networks

Link Encryption

- Protects entire circuit

Encrypt → Tunnel → Decrypt

IPSec

End-to-End Encryption

- Protects comms b/w two parties

client — server

TLS 1.2
SSH

Wireless Security

WEP

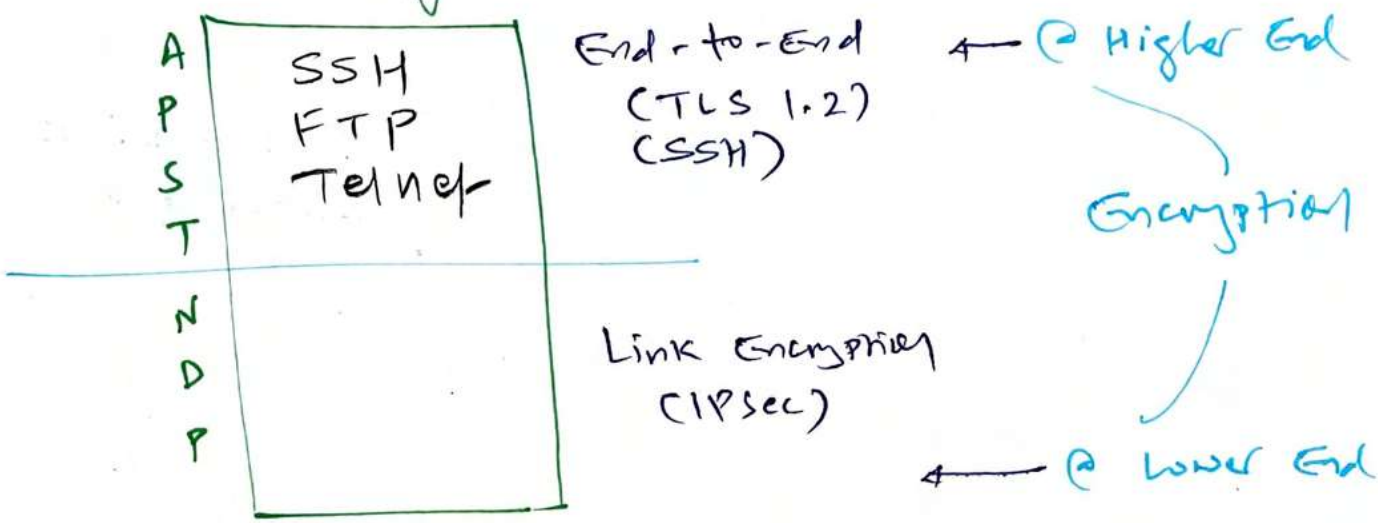
- 64 & 128-bit encryption
- Not secure

WPA

- Eliminates weakness of WEP with TKIP

WPA2 uses Temporal Key Integrity Protocol AES Cryptography

OSI layers



* IPSec

- Uses public key cryptography
- Provides Encryption, access control, non-repudiation & message authentication using IP Protocols.
- Prime use: VPN
- 2 operations

  - Transport mode (P2P)
    - only packet payload is encrypted. Good for P2P.
  - Tunnel mode
    - Entire packet + header is encrypted
    - Ideal for gateway to gateway comms.

- IPSec relies on Security Associations (SA)

  - AH
    - Authentication Header
    - Provides message integrity, non repudiation, access control to prevent replay attacks.
  - ESP
    - Encapsulating Security Payload
    - provides confidentiality & integrity of message
    - Limited encryption & Authentication to prevent replay attacks.

IPSec runtime

→ Creates SA

- To represent communication session
- Record configuration about session

Requires 2 SA for bi-directional

ISAKMP (manages SA)

- Internet Security Association & Key mgt protocol
- ISAKMP: provide background support for IPSec
  - → Negotiate, establish, modify & delete SAs

4 requirements.

1. Authenticate communicating peers
2. Create + manage SAs
3. Provide key generation mechanisms
4. Protect against threats: DDoS, Replay.

CRYPTOGRAPHIC ATTACKS

↳ Analytic Attack

↳ side channel Attack (Timing Attack)
- stalk her to find out where she work, what she does for living.

↳ Implementation Attack - Exploits (implementation flaws)
↳ E.g Heartbleed Bug + Reverse Engr.
↳ SCA (Source code Analysis), most common method to find

↳ Statistical Attack (Frequency Analysis Attack)
- identifies the pattern

↳* Brute force
- Randomly find correct cryptographic keys
- KL is important

Enhanced Attack : Rainbow Table

Use cryptographic SALT

Password	Random number

↳ ~~Frequency Analysis~~ Ciphertext only Attack

Attacker has ciphertext & their goal is to find key used in Encryption process

↳ * Known plaintext : Attacker has copy of

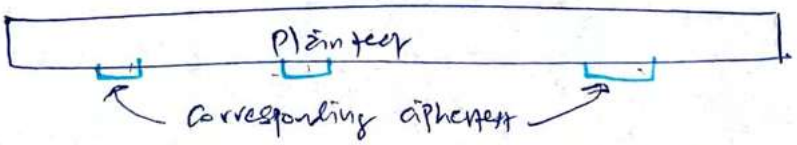
(ciphertext)
Encrypted + plaintext message

→ To know the key how ~~to generate~~ cipher text generated from

↳ Chosen ciphertext

Attacker : Ability decrypt portions of cipher = to know key

↳ Chosen Plaintext



Attacker : Ability to extract plaintext portion to determine which encrypted algorithm is used.

↳ Man in the middle
↳ RDES is vulnerable for this.

↳ * MitM (man in the middle) — Attacker establish secure connection to client & to all comms to legitimate server goes via his machine.

prevention:

↳ Birthday
A.K.A — collision or Reverse Hash matching
— To find if different msg produce same message digest

↳ * Replay → malicious user intercepts encrypted message b/w two parties & Replay the captured message to open new session.

pass the hash
p.to end

Prevent using expiration of msg or incorporate timestamp.

To Secure Email

PGP

- Pretty Good privacy
- Combines CA hierarchy with "Web of trust" concept
  - you have to (must) become trusted by one or more PGP users to begin using the system.

* 2 versions of PGP

Commercial

- Use RSA for key exchange
- IDEA for Encryption/Decryption
- MD5 for digest production

Freeware

- Use DH for key exchange
- Use CAST 128-bit Encryption/Decryption
- Use SHA-1 hashing function

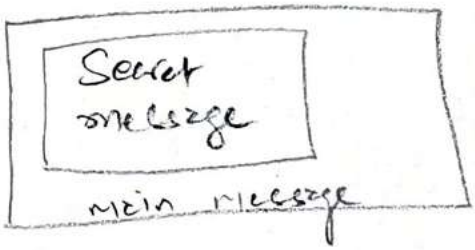
S/MIME

- Secure/Multipurpose Internet Mail Extension
- Uses RSA Encryption Algorithm
  - O365
  - Lotus
  - Mac OS X mail
  - Mozilla Thunderbird
- Relies on X.509 for exchanging cryptographic keys
- RSA is only Public key cryptographic protocol supported by S/MIME

most facinating approach

- Web Browsers & web servers use private/public key with Asymmetric cryptographic approach but web browser uses Symmetric keys for speed.
  - this is awesome (OSM P257)

Steganography



Art of using cryptographic technique to embed secret message within another message.

Brute-force Attack

- Use salt
- longer key length
- Key stretching

Weak factor — if any of below is element is weak, attacker can break the cryptosystem

1. Algorithm without flaws
2. Large key size
3. protect the secret key

Pass the Hash – Replay Attack

↓

Targets AD.

Countermeasures

- Timestamps
- Sequence Numbers

10. Physical Security Requirements

Purpose of Physical Security :: Protection against physical threats.

- Smoke
- Fire
- water
- Storm

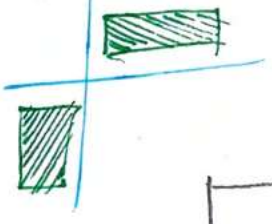
Earthquake

Theft
Equipment failure
Personal loss

Vandalism, Explosion, Building collapse

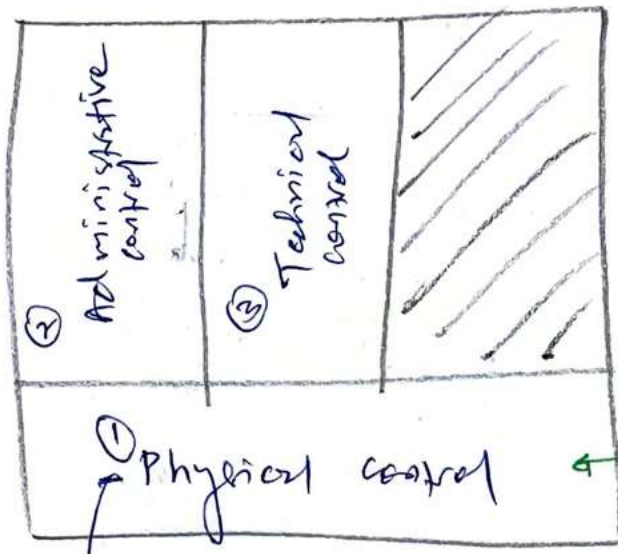
Toxic material using loss.

PERSPECTIVE



Identify Physical Threats ⟹ Implement safeguards

Apply Security Principles To Site & Facility Design



First line of defence, People are last.

Start with Designing Secure Facility + operations

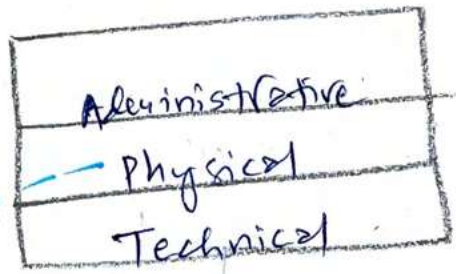
- Secure Facility Plan
  - Developed through critical path Analysis
    - what to secure?
- Site selection
- Facility Design
  - Crime prevention through Environmental Design (CPTED)
    - guidelines to design physical structure environment
- visibility
- Natural disasters

- Technology Convergence
  - Provide efficiency + cost saving but watch-out for single point of failure
  - when technology merge over time
    - e.g. single connection for voice, vide, data = SPOF

IMPLEMENT SITE & FACILITY SECURITY CONTROLS

Physical Security perspective

Access control perspective



Remember below order when implementing Security for physical Environment.

1. Deterrent – Fencing
2. Denied – Locked Door
3. Detect – Sensor Alarms
4. Delay – Enough control to delay while police is on the way.

* Equipment Failure

One day it will = Prepare mentally for AVAILABILITY.

Response time to return system to Functional level $\propto$ cost involved in to maintain that Solution

if onsite replacement $\neq$ Feasible

⇩

Lock SLA with vendor.

Aging Hardware = schedule for replacement / repair

MTTF (Mean time to failure)

- Router last for 10 years

Replace device before MTTF expires

MTTR (Mean time for Repair)

- Router needs repair / maintenance every 1 year

MTBF (Mean time between failures)

- Estimation of time between first and subsequent failures

while device sent for replacement, Prepare alternate / Backup Hardware

* wiring closet
(Intermediate distribution Facilities - IDF)
(Premise wire Distribution Room)

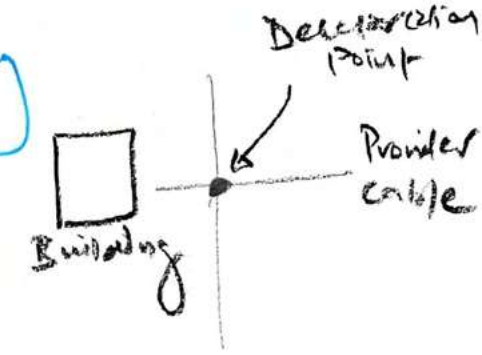
→ Physical security Focus ⟹ Prevent Unauthorised Access

→ Have wiring closet security policy ⟹ Provide to Building mgmt staff

Element of

Cable Plant Management Policy

→ Entrance Facility

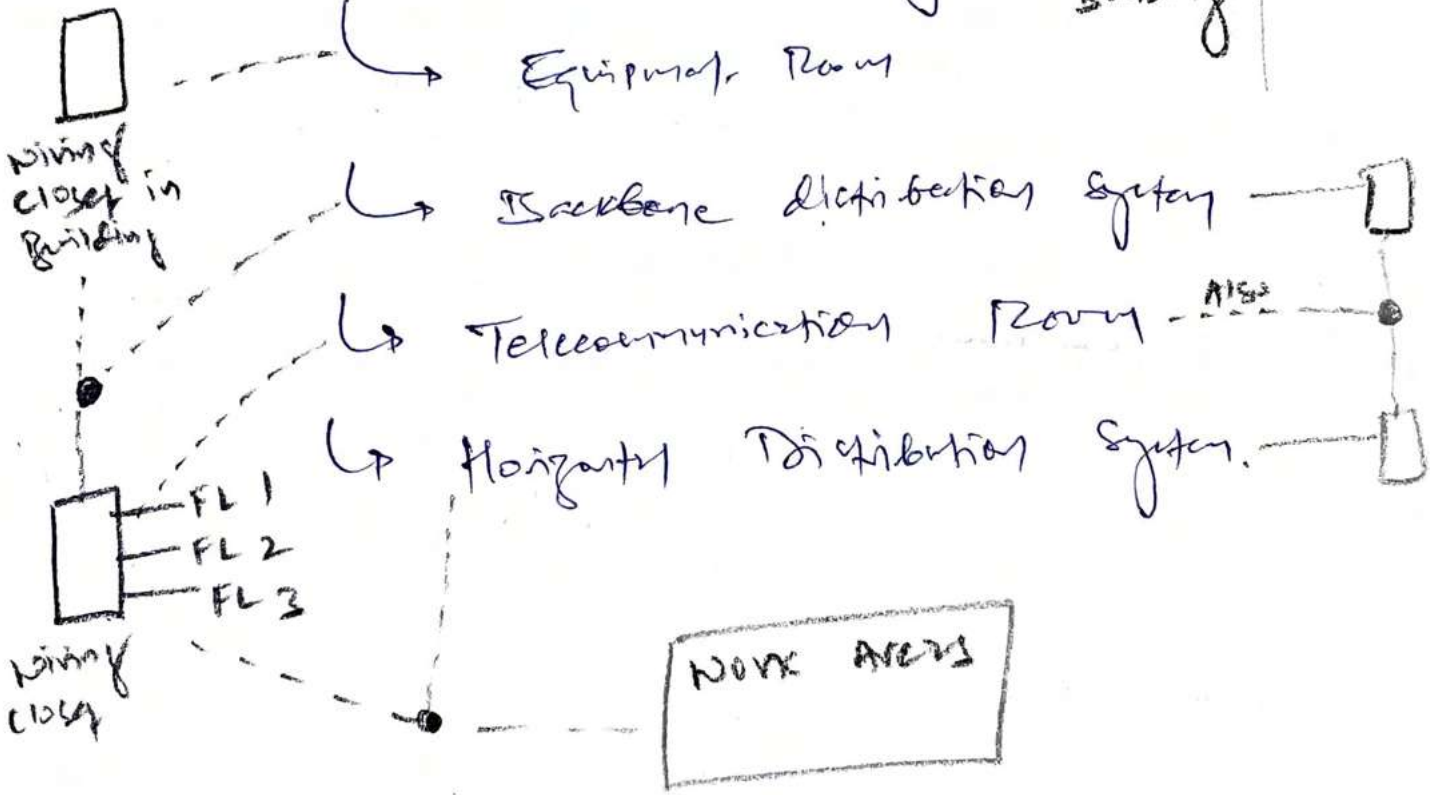


→ Equipment Room

→ Backbone distribution System

→ Telecommunication Room

→ Horizontal Distribution System.



E-E

Wiring closet security concern = Prevent physical Unauthorised access

→ Update building mgmt about wiring closet security policy

* Server Rooms / Data Centers

- can be human incompatible
  = low temp, low light
- Don't put on ground Floor / Basement = should be at care of building (heart)

Technical controls for Datacentre

Smartcards
- Used for Authentication purpose
- mostly for multi-factor: "something you have"

IDS
- only useful when connected to intrusion alarm
- 2 aspects of IDS
  (a) How it gets power
  (b) How it communicates
  - Battery Backup
  - Heartbeat sensor

Proximity Readers
- Passive device
  - NO electronics
- Field-power Device
  - Has electronic, activates when device enters to electromagnetic field
- Transponder device = self-powered & transmit signal
  - Garage Door Remote

Access Abuse

- Piggybacking
- Masquerading
  - Using someone else' security ID

Prevention:
- Audit trails + access logs are helpful
  - manual
  - Automatic
- CCTV + security guards.

Emanation Security

TEMPEST

Read ch: 9 Electromagnetic Radiation for Basics / Intro

Called TEMPEST countermeasures

Safeguards to Protect Emanation Attacks

- Faraday cage
  - Box
    - mobiles / TV Broadcast don't work here
  - Blocks Electromagnetic signals (EM)
- White Noise
  - Broadcasts false traffic in the time to mask and hide the presence of real emanations.
  - White Noise
    - non-confidential signal (fake signal)
- Control Zones
  - outside control zone, Emanation is blocked
  - within control zone, EM signals are supported.

* Media Storage Facilities

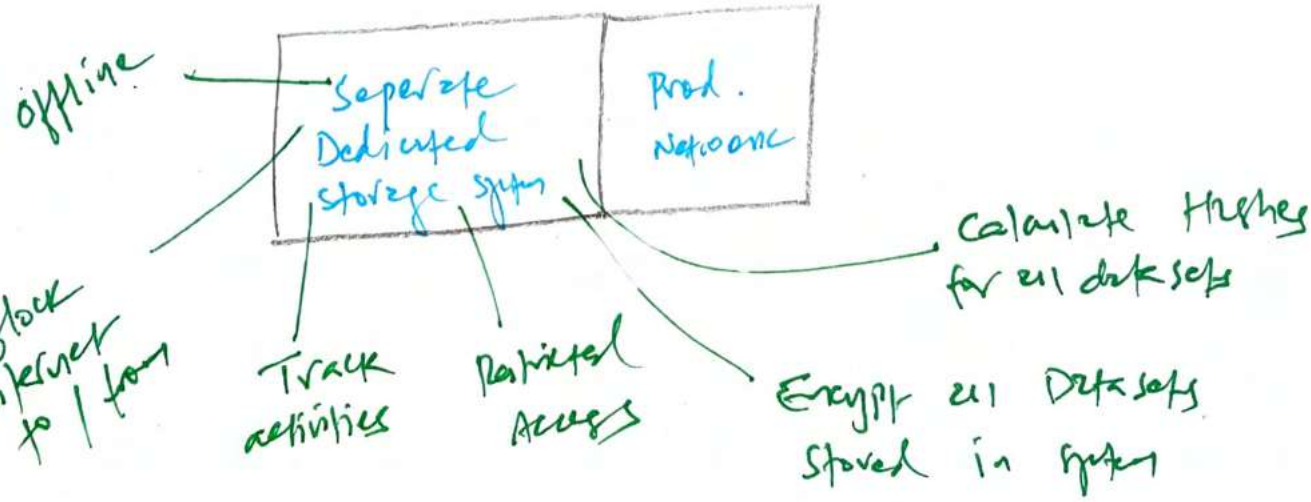
Security concerns
- theft
- corruption
- Data Remnant Recovery

(To Reduce Risk)
How to secure media storage?

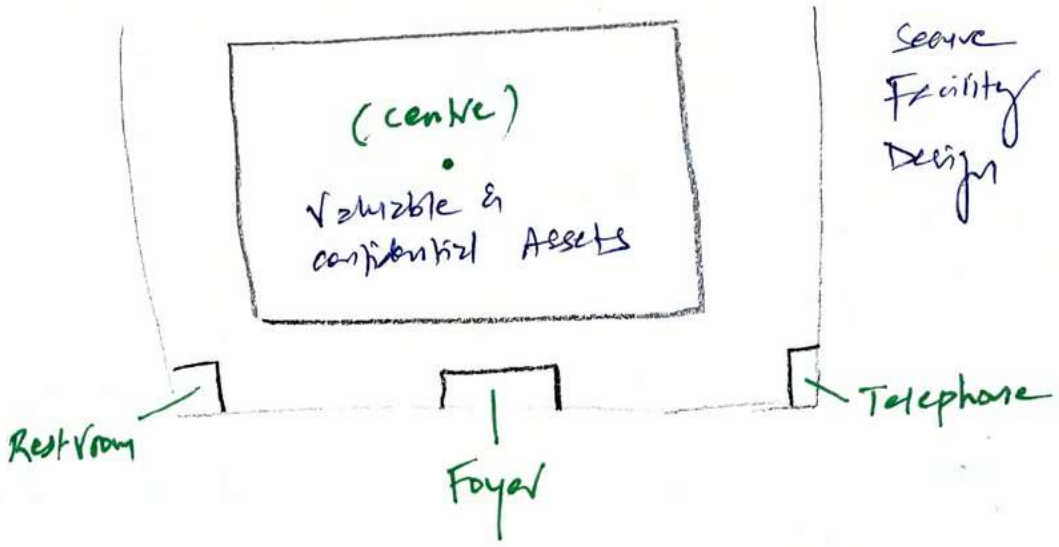
- Physical security (from stealing)
  - locked cabinet
- Higher protection
  - Fire, Flood, EM field, Temp monitoring
- From Malware
  - Patching
- Secure Wiping (Avoid Data Remance)
  - Zeroization
    - Erase data by replacing with zeros
- Restrict Access
- Lable media
  - classification
- Verify media with Hash-based integrity
  - To ensure valid file remains valid

* Evidence storage

Cyber crime ↑↑↑ ⟹ Retain logs, audit trails & records of digital events.



* Restricted and Work Area Security



Secure Facility Design

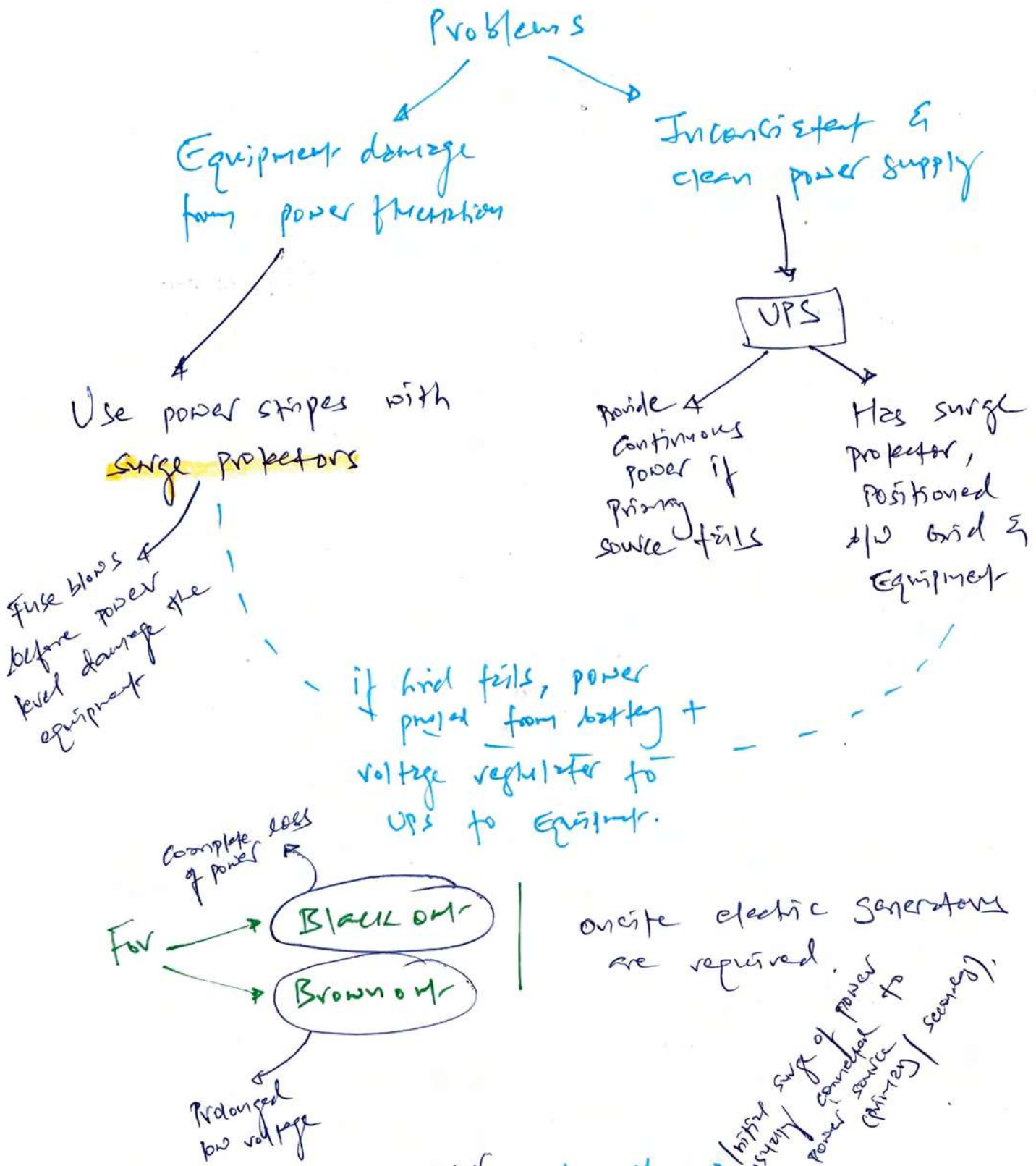
Something to consider

- Wall partition to avoid shoulder surfing
- Classified work Areas (similar to data & Asset)
  - only personnels with valid clearance can access
- Address visitors & visitor control
- Physical security.
  - RFID ID
  - Cameras
  - Mantrap
  - CCTV
  - written logs
  - Keys / locks

Sensitive Compartmented Information Facility (SCIF)

- Concept for restricted work area
  - military
  - government
- No photography, video allowed
- Purpose: Provide restricted access to only those with fitness need based on clearance level
  - store, view & update sensitive compartmented information (SCI)

* Utilities and HVAC Considerations



* Noise

→ from Equipment = Affect Data Transmission

- Telephone
- TV
- Computer
- Radio / Audio
- Network mechanisms

Noise

2 Types of Electromagnetic Interference (EMI)

Noise

Common mode noise

- Generated by difference in power b/w hot & ground wire of power source

Traverse mode noise

- Generated by difference in power b/w hot & neutral wire of power source

Noise

Radio Frequency Interference (RFI)

- All electronic appliances generate RFI

So far prob. Equipment from

- Power loss
- Noise

* Temperature, Humidity & Static

→ 15 to 23°C (60 to 75 °F)

DC — 40 to 60%.

Too much humidity → corrosion / moisture / Equipment Damage

Too little humidity → static electricity

(static voltage)
Static electricity → 2000 volt = system shutdown

4000 = printer jam

17,000 = permanent circuit damage

Min. level of static discharge can destroy electronic equipment.

* Water Issues

- leakage
- flooding

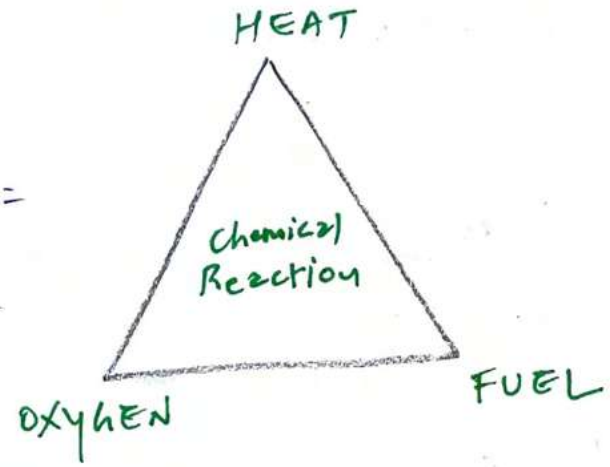
Water + Electricity = danger (Serious risk of Electrocution)

- Install water detection circuit
- Be familiar with shutoff valves & drainage locations.
- Monitoring for plumbing leaks.

* Five prevention, Detection & Suppression

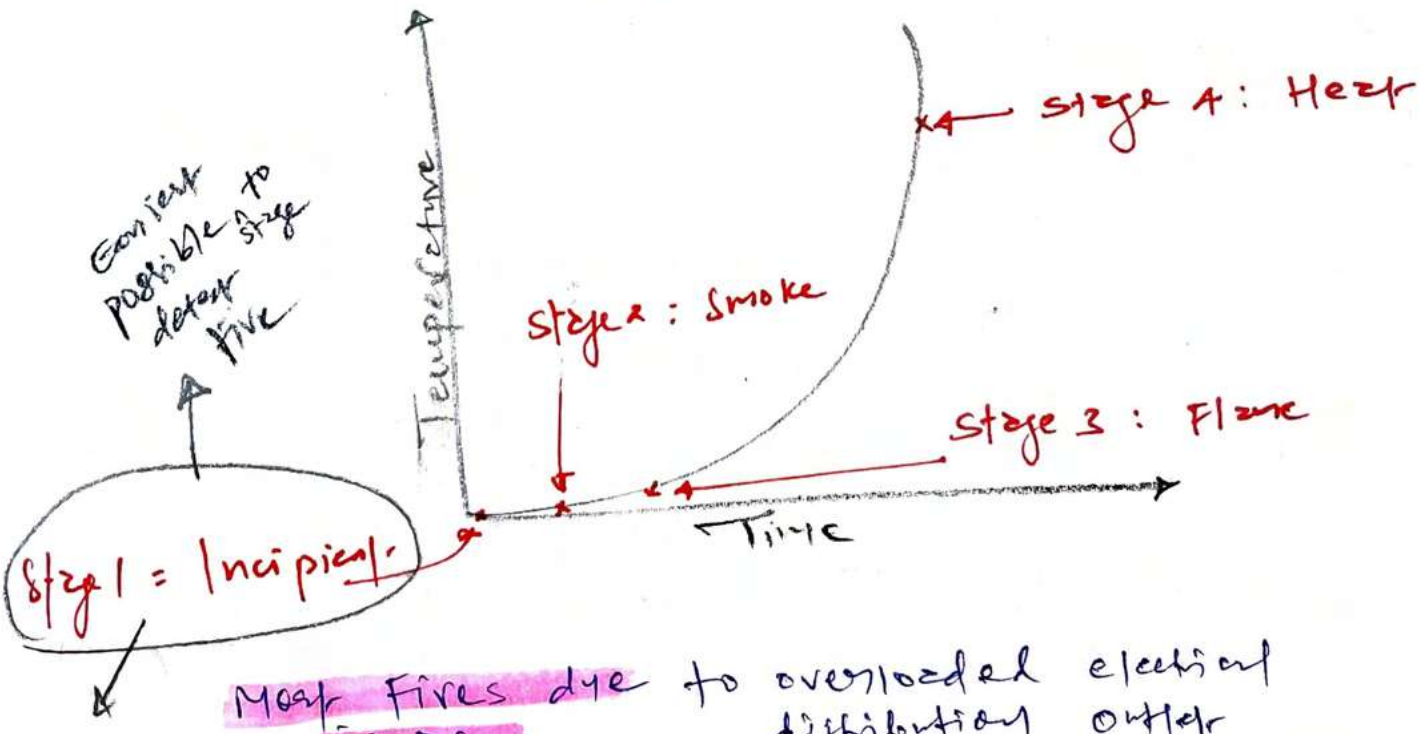
The Five Triangle

- Remove any one of four = fire can be extinguished



Various suppression mechanism exist but consider what aspect of fire triangle it addresses

Stages of FIRE



Most fires dye to overloaded electrical distribution outlet

Fire Mgmt → Evacuation route (at least two)
→ Awareness Training (Suppressing mechanisms)
→ Use of Fire Ex.

only when Ionization no smoke

* Five Extinguishers

→ only use in Incipient stage

By Types

A
Common Combustibles
Water, Soda Acid, Dry Powder

B
Liquids
CO_2, Halon, Soda Acid

C
Electrical
CO_2, Halon

water can't used for class B or C

D
Metal
Dry powder

Oxygen suppression can't use on metal fire because metal produces its own oxygen.

* Five Detection Systems

→ To prevent Fire

- Automatic Detection
- Suppression System

Fixed-Temperature Detection System

Triggers when specific temp is reached.

Rate-of-Rise Detection System

Triggers suppression when the speed at which temp reaches to specific level.

23° → 38°

Flame-Actuated System

Suppression based on infrared energy of flames.

Smoke-Actuated System

Use of photoelectric or radioactive ionization sensors as triggers.

* Water Suppression Systems

most common cause = Human Error

4 Types

Wet Pipe System (closed head)
- Pipe full of water discharge when triggers suppression

Dry Pipe System
- Filled with compressed air
- Suppression trigger to escape air = open valve = fill the water

Deluge System
- Large dry pipes but bigger
- Not ideal for offices that has electronics & computers.

Preaction System
- Combination of Dry + wet pipes
- Dry in the initial stage (2 steps) of fire, then filled with water

Best for environment that house computers & Humans together.

Used for Sprinklers head heat activation before dispensing water

* Gas Discharge Systems

└ Removes oxygen from air = Don't use where people are located.

Halon = Effective fire suppression compound but becomes toxic @ 900°F

Use substitutes
- FM-200
- CEA-410
- NAF-S-III
- FE-13
- low pressure water mist
- Argon / Argonite / Inergen / Aero-K

* Damage caused by Fire

Smoke

- Damage magnetic storage device

Heat

- Damage any electronic or computer component

Suppression media

- cause short circuit
- initiate corrosion
- render equipment useless

Implement & Manage Physical Security.

Designate Facility Areas As

- Public
- Private
- Restricted

Physical Access controls — Monitoring — Prevention Mechanisms

* Perimeter Security Controls

- Fence
- Gate
- Turnstile
  - Revolving Door
- Mantrap
  - Prevents piggybacking
  - Remember NIAS9
  - Delay Feature
- Security Bollards
  - Prevents vehicles ramming access points.

* Lighting — ~~Security lights~~ — Light poles should be placed the same distance apart as diameter of illuminated area

* Security Guards & Dogs

Guards
- Vulnerable to social Engg Attack
- + they are expensive

Dogs
- Most effective as deterrent & detection.

* Internal Security Controls

Escort assigned to visitors.

Monitor their access + activities closely.

Keys & Combination locks

- Access to individual entry (storage, cabinets)
- + Key card for shared Entry points (Building)

Badges

- Simple ID with photo
- smart-card as multifactor AAA

Preset locks

Programmable + combination locks → more control

Anybody can pick the lock, called Shimming.

Motion Detectors (MD)

- Infrared or (heat-based MD heat level & Patterns
- Wave pattern motion (transmit constant ultrasonic signal
- Capacitance motion detector (changes in electrical or magnetic field)
- Photoelectric MD
- Passive Audio MD (listen to Abnormal sounds)

Intrusion Alarms

changes in light, for dark rooms

Alarm Types:
- → Deterrent Alarm
- → Repellent A.
- → Notification A.

Alarm Categories:
- → Local Alarm System
- → central station System
- → Auxiliary station

P.t.o (cont...)

Secondary Verification Mechanisms — to get rid off false positives

Sensors
Alarms ⇒ False Alarm (Bird, Animal)
MD

Need more than one triggers to confirm

E.g CCTV = secondary mechanism
- Need manual review after trigger

CCTV is preventive measure.
Reviewing footage is detective measure.

Environment and Life safety

Physical security
└ primary focus
- Protect human life

└ Secondary focus
— Restore IT system

* First Protect people. Bcp comes later.
— OEP (occupant emergency plan) used to minimize threat to life

Privacy Responsibilities & Legal Requirements

Safety of PII ← Address in organization's security policy

NIST 800-122

Privacy = Protecting PII from unauthorised Access

GDPR from EU

Regulatory Requirements

Country / jurisdiction	Industry (BANK, HEALTH CARE)
Legal Requirements	

Foundation of security framework

Notes

↳ Soda Acid : Extinguishers work to remove fuel supply
+ other dry powders :

↳ Water : Suppresses the temperature

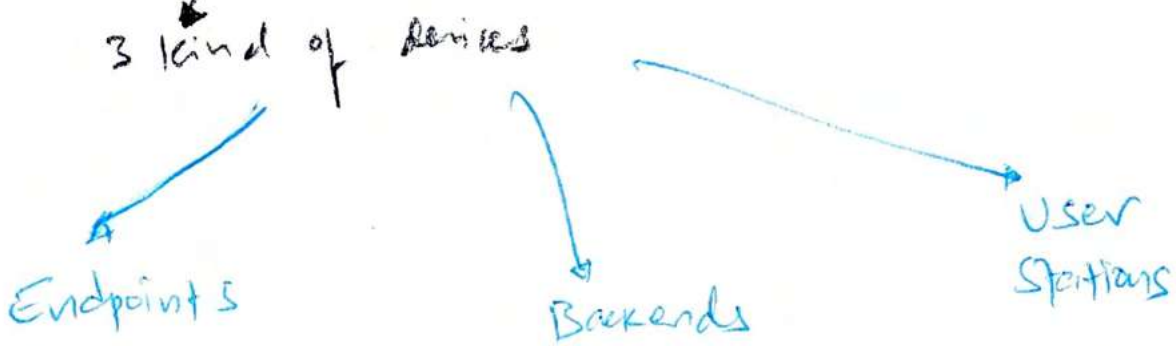
↳ Halon & CO_2 : Remove oxygen supply from fire.
is Bad / Banned

↳ Humidity : DC range 40 - 60 %.
lower = static electricity
high = moisture / Equipment Damage

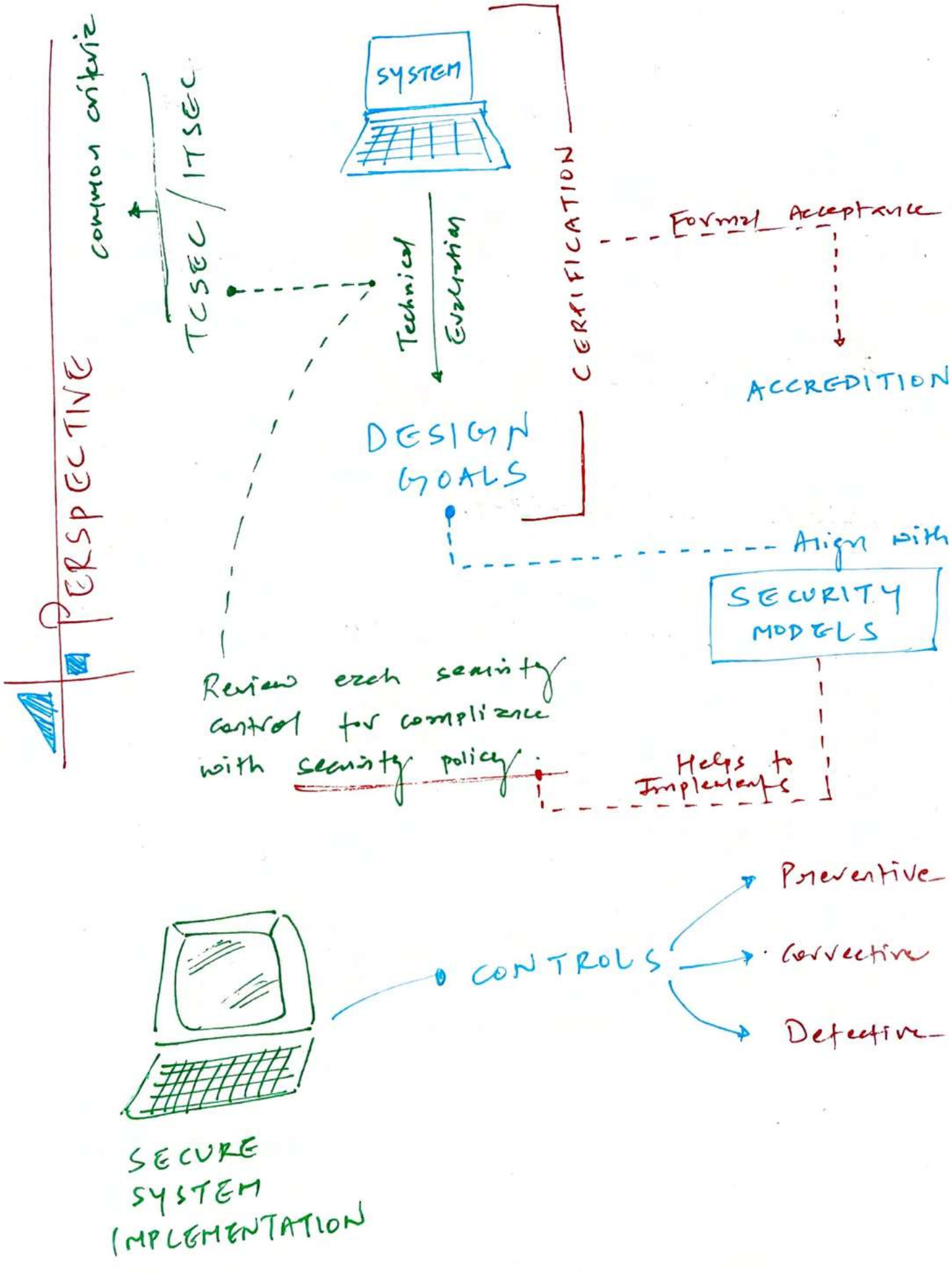
↳ Capacitance : Type of motion detector that monitor the electromagnetic field in monitored area, it senses the disturbance that corresponds to motion.

→ Halon use CFC suppressant material that was banned in Montreal protocol because it depletes ozon layer.

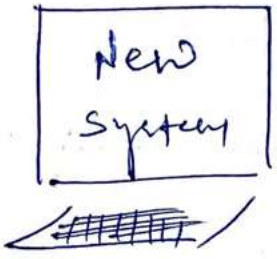
SCADA - Supervisory Control and Data Acquisition



CH: 8 PRINCIPLES OF SECURITY MODELS, DESIGN, AND CAPABILITIES



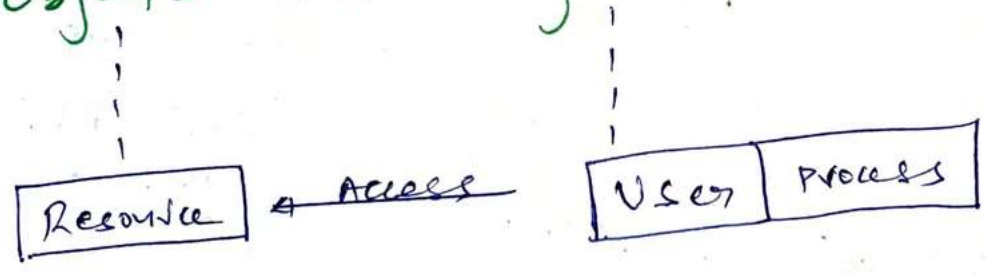
IMPLEMENT & MANAGE ENGINEERING PROCESS USING SECURE DESIGN PRINCIPLES



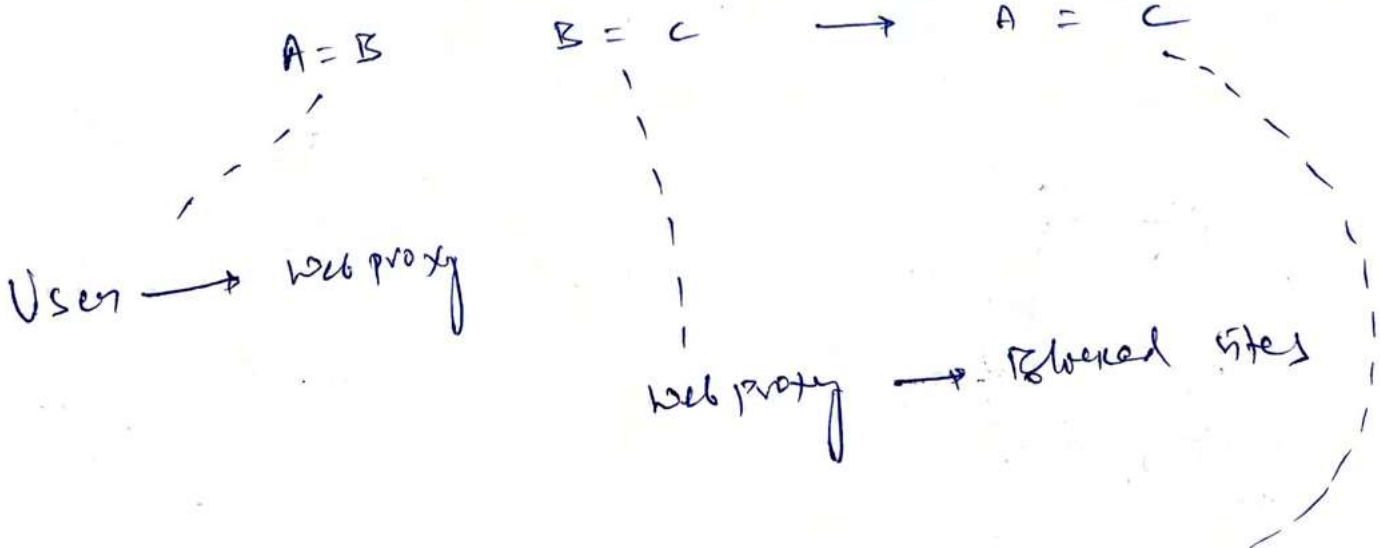
Build security : EASY

Add security : DIFFICULT

* objects and subjects



Transitive trust = serious security issue



* closed and opened Systems

- Proprietary + same manif.
  + Not easy to integrate
  - Secure

- Industry standard + Easy to integrate
  - Not secure

Open Design Methodology – refers to Kerchoff's principle –
Security of design shouldn't be secret like cryptosystem – this approach of open design provides independent security confirmation

* open-source vs. closed-source

- open-source
  - LINUX
  - Internal logic + source code open to public
- closed-source
  - WINDOWS
  - Hidden from public

Both can be either open or closed system.

* Techniques for ensuring CIA

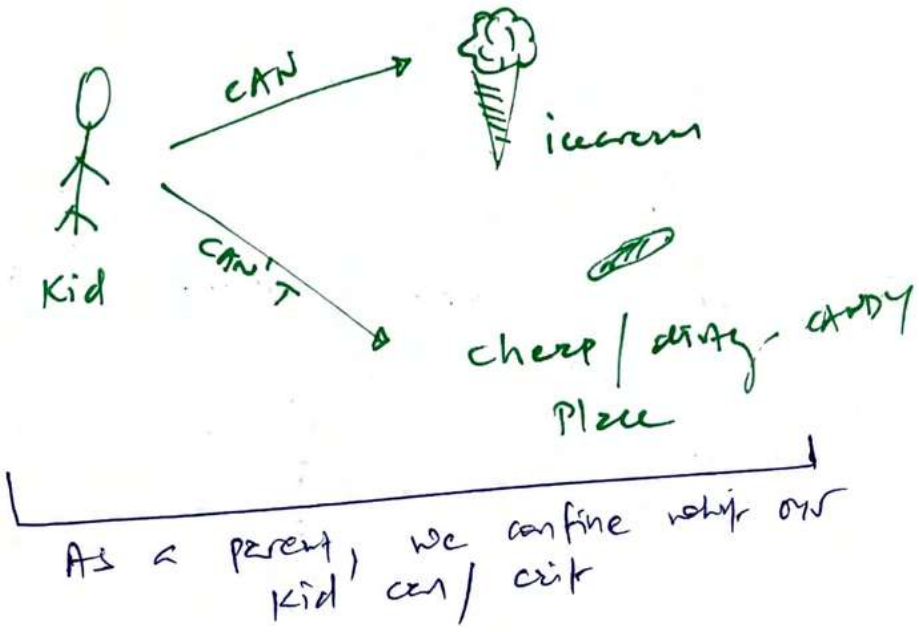
(from s/w designer/ perspective but applies program to all areas of security)

- Confinement
- Bounds
- Isolation
- Controls
- Trust & Assurance

CONFINEMENT --- Sandboxing

- Restricts a process or software program to reading from or to certain memory locations.

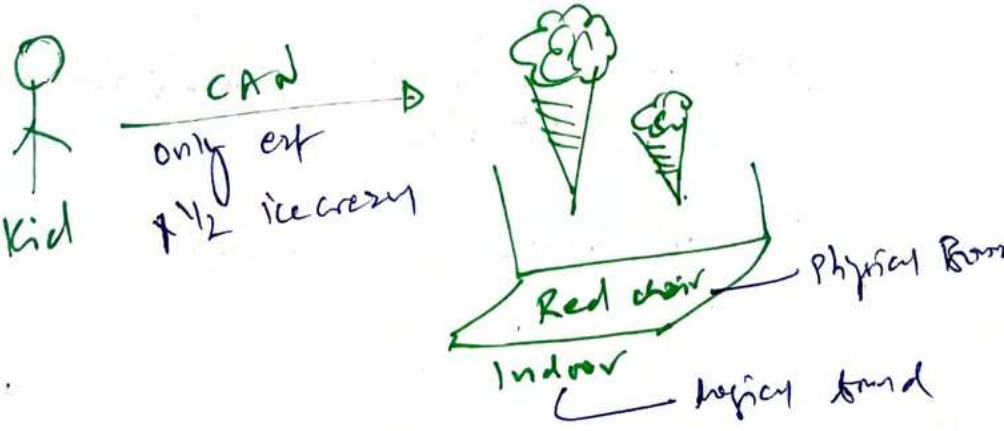
Confinement in s/w development is concept of isolation to ensure that running process / Application cannot interact with other entities unless authorized to.



BOUNDS --- physical --- logical

- Bounds are the limits of memory a process cannot exceed when reading or writing.

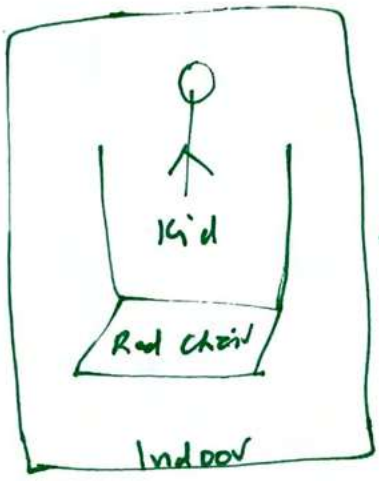
Bounding checking restricts a process to specific areas of memory and prevents external inputs from interaction.



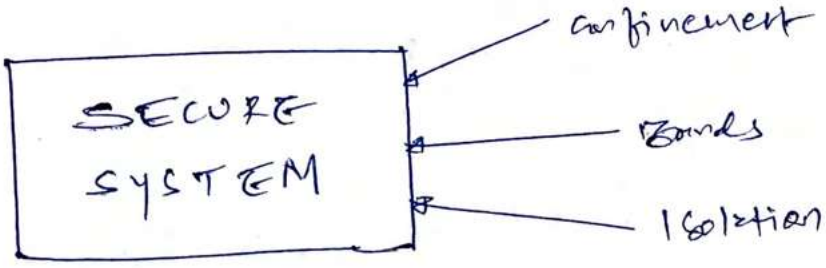
- Bound is that area where process (kid) is already confined.

ISOLATION ---- mode

- where process is confined with memory bound.



<---- isolated | safe from external toxic environment



CONTROLS ---- MORE Ch: 14, 629-633

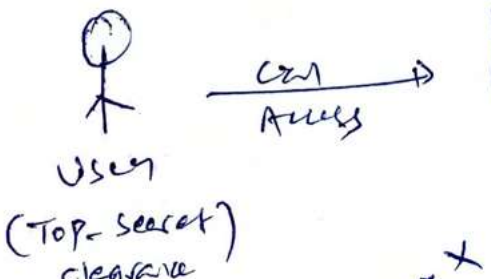
- check Access control matrix model for example

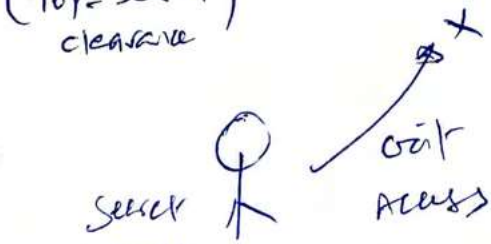
DAC

- All objects have owners
- owner have full permission
- owner can also delegate to data custodian for day-to-day operations.

MAC - (p.1.0 End)

- Subjects & objects have labels / classification





GOAL

- To limit access to object & subject
- To protect confidentiality & Integrity of data

TRUST & ASSURANCE

SECURITY → ✗ Not an Afterthought

↓ ✓

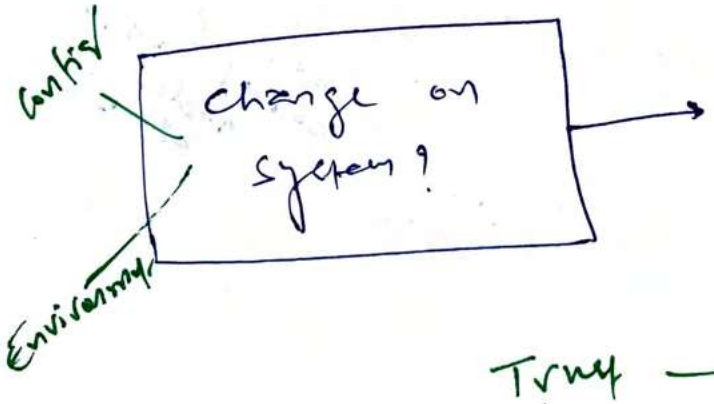
Building
(once security integrated to design)

IT MUST BE

Design → Engineered → Implemented → Tested → Audited → Evolved → Certified → Accredited

so far I did this

now



Trust — Assurance

Trust: Implementing specific security features for the system

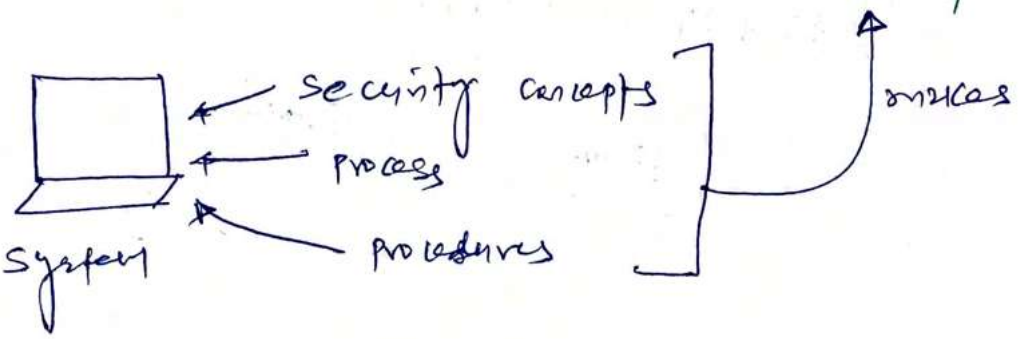
Assurance: Assessment of reliability & usability of security feature in real world situations.

TRUST BUT VERIFY.

Never trust. Always verify. ZERO TRUST

FUDAMENTAL CONCEPSTS OF SECURITY MODELS.

- Provide a way to formalize SECURITY POLICIES.



These models offers deep understanding on how OS should be designed & developed to support a specific security policy.

Tokens → Every object is seperate token associated with resource. Token has security information about object prior accessing access to actual object.

Capabilities → ~~Table, that which subject can access which objects.~~ Row that maintains ~~security attributes~~ for controlled object

Security Labels → Permanent label attached to object, can never altered.

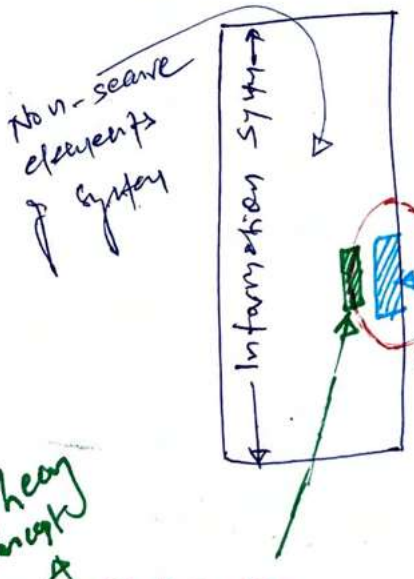
→ Provides safeguard against tampering that token & capabilities never provide.

* TRUSTED COMPUTING BASE (TCB)

orange book / TCSEC
(Trusted computer system Evaluation Criteria)

P.T.O END for REF. MONITOR CONCEPT

Software + Hardware + controls ⟹ forms ⟹ TCB ⟹ Enforce ⟹ Security Policy



1. STATE MACHINE MODEL

Always boot in secure state

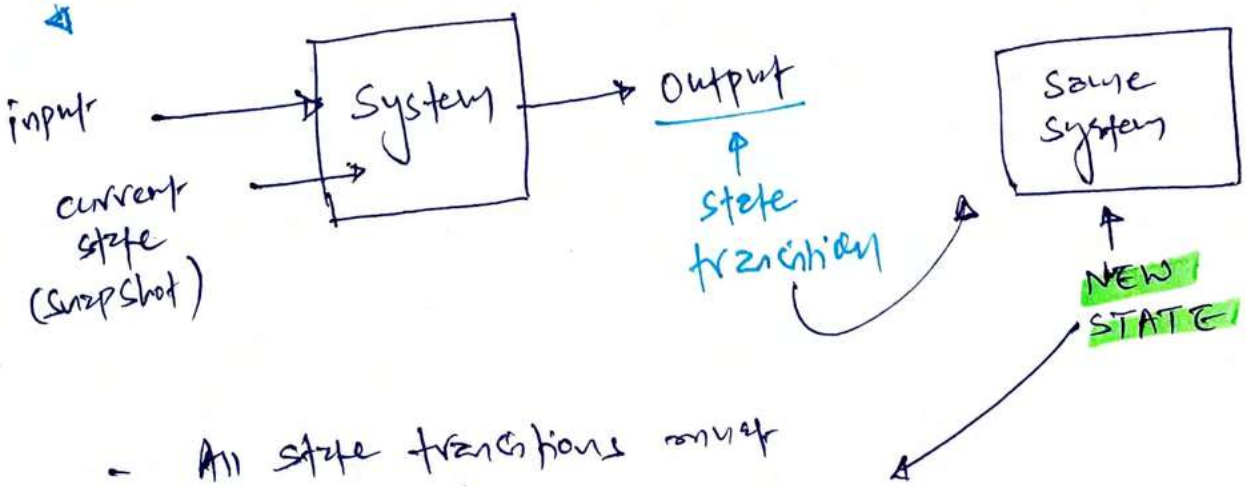
All instances of subjects → MUST BE SECURE → objects

Based on FSM (Finite State Machine)

- system is always secure, no matter which state is in

Snapshot of System = Requirements of security policy

Secure system



- All state transitions must be evaluated.
- New state will be checked against security policy, if it's compliant = secure state.

2. INFORMATION FLOW MODEL

Biba
Bell-La Padula

Prevents → Unauthorised
Prevents → Insecure
Prevents → Restricted

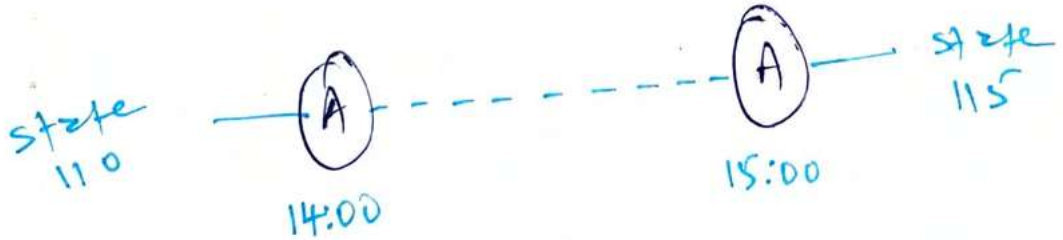
Information Flow. b/w diff. level of security

Model Focus → Information flow
Model Focus → Type of flow.
Model Focus → Address COVERT CHANNEL by excluding nondefined flow pathways.

Allows authorised information flow b/w subject & object within same classification or different classification level.

Interesting

Establish relationship b/w two ~~object~~ versions of state of same object at different point of time.



→ Biba + Bell-La Padula = MAC Models

* 3. NON-INTERFERENCE MODEL.

Action of Subject A : Higher classification → should not affect X

Action of Subject B : Lower classification

Provides protection

← if this happens, Subject B will be placed into insecure state

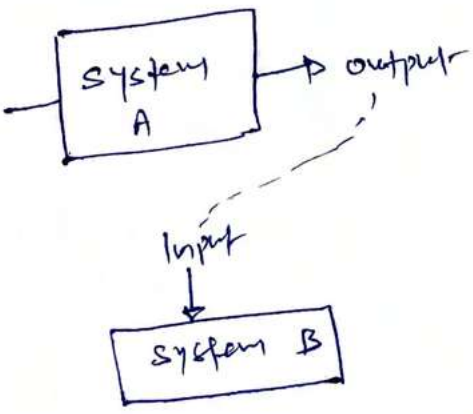
→ This type of information leakage creates COVERT CHANNEL

---

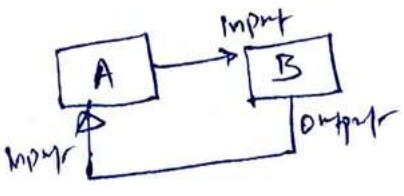
* Composition Theories

- Kind of information flow model
- Info. flows of 2 systems rather than individual system

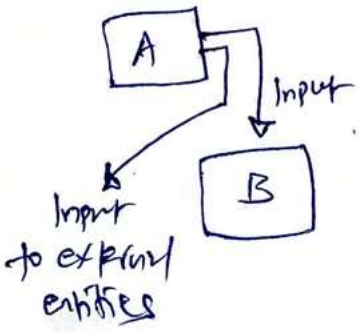
Cascading



Feedback



Hookup



4. TAKE-GRANT MODEL

Focus: Dictates how rights are passed from one subject to another or from subject to object.

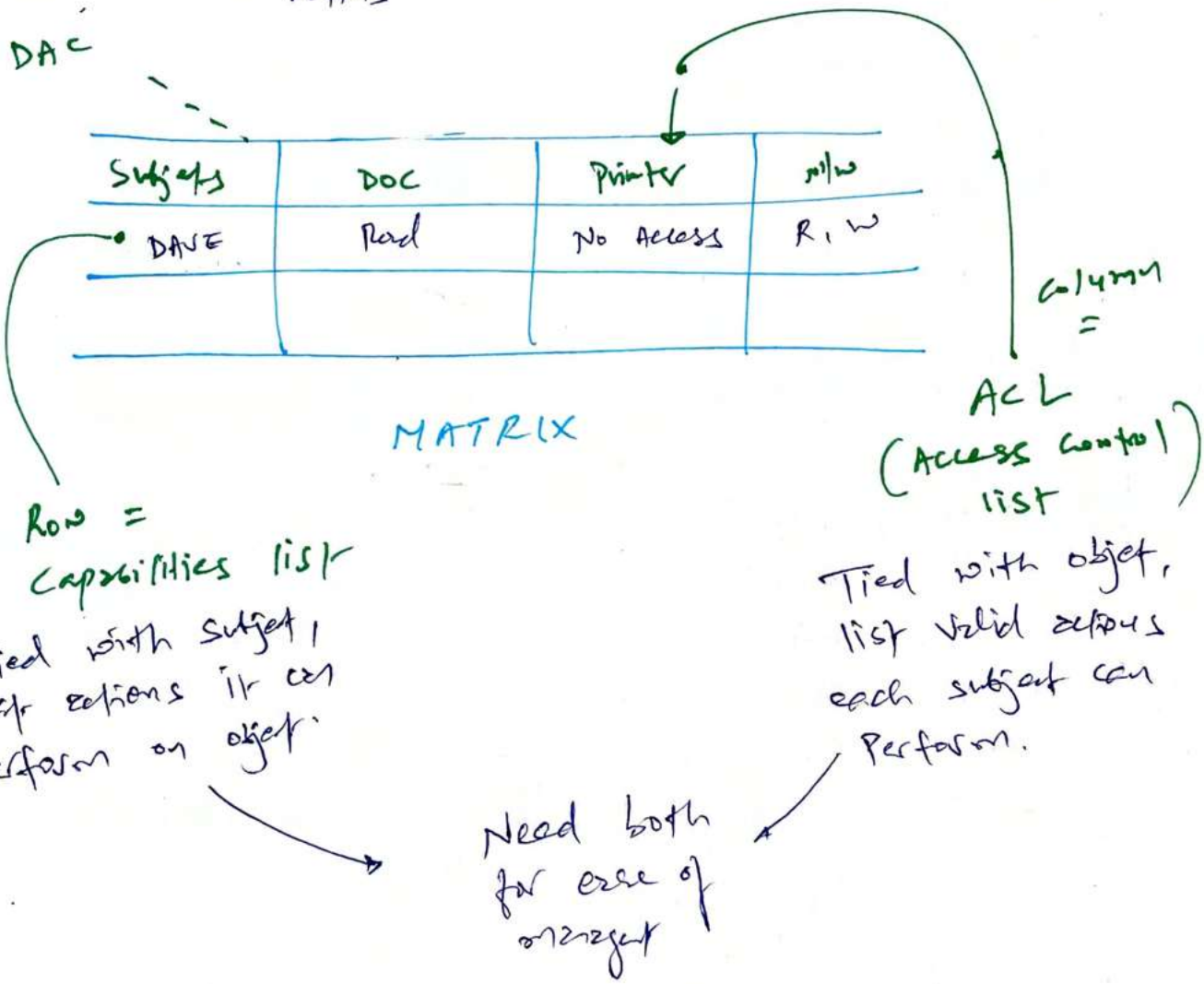
2 Rules

- Take Right
  - from subject to other subject / object
- Grant Right
  - from subject to other subject / object

Subject → Subject
Subject → object

5. ACCESS CONTROL MATRIX

Just a table, lists all subjects & objects. What subject can perform on objects
↑ actions



Column → Object

Row → Subject

FIRST REMEMBER THIS

6. BELL-LAPADULA MODEL

Addresses only confidentiality of Data

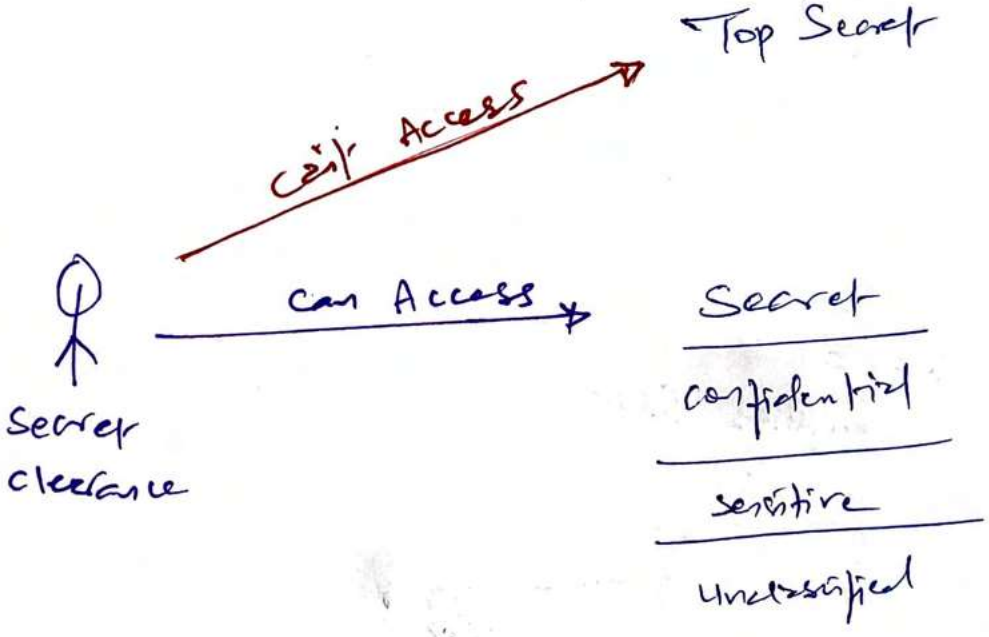
Info. Flow model

state machine concept

for Federal

→ To protect classified information

- Prevents information flow from low to high security level.



- Prevents information leak from classified level to less secure clearance levels.

HOW!

Higher classified objects

BLOCKS

lower classified Subjects

bell-lepadula (contd.)

Employs STATE MACHINE Concept

LATTICE CONCEPT

3. PROPERTIES To maintain confidentiality

1. Simple security Property — can read at your level and below but not up

NO READ-UP

2. * (star) security property (confinement property)

NO WRITE-DOWN — can write at your level and up but not down

Prevent information leakage from top to bottom

3. Discretionary security Property (strong *) — only read and write into into your own security level - no up or down

Enforce DAC

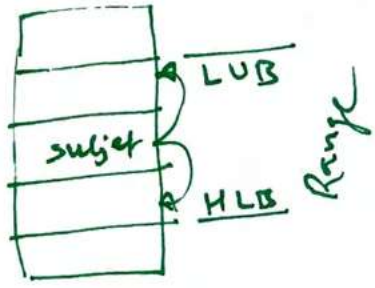
Enforce subject need to know basis in order to access object based on access matrix

- Only supports "C", no "I" & "A"
- Assumes security transitions b/w layers
- No support for covert channel.

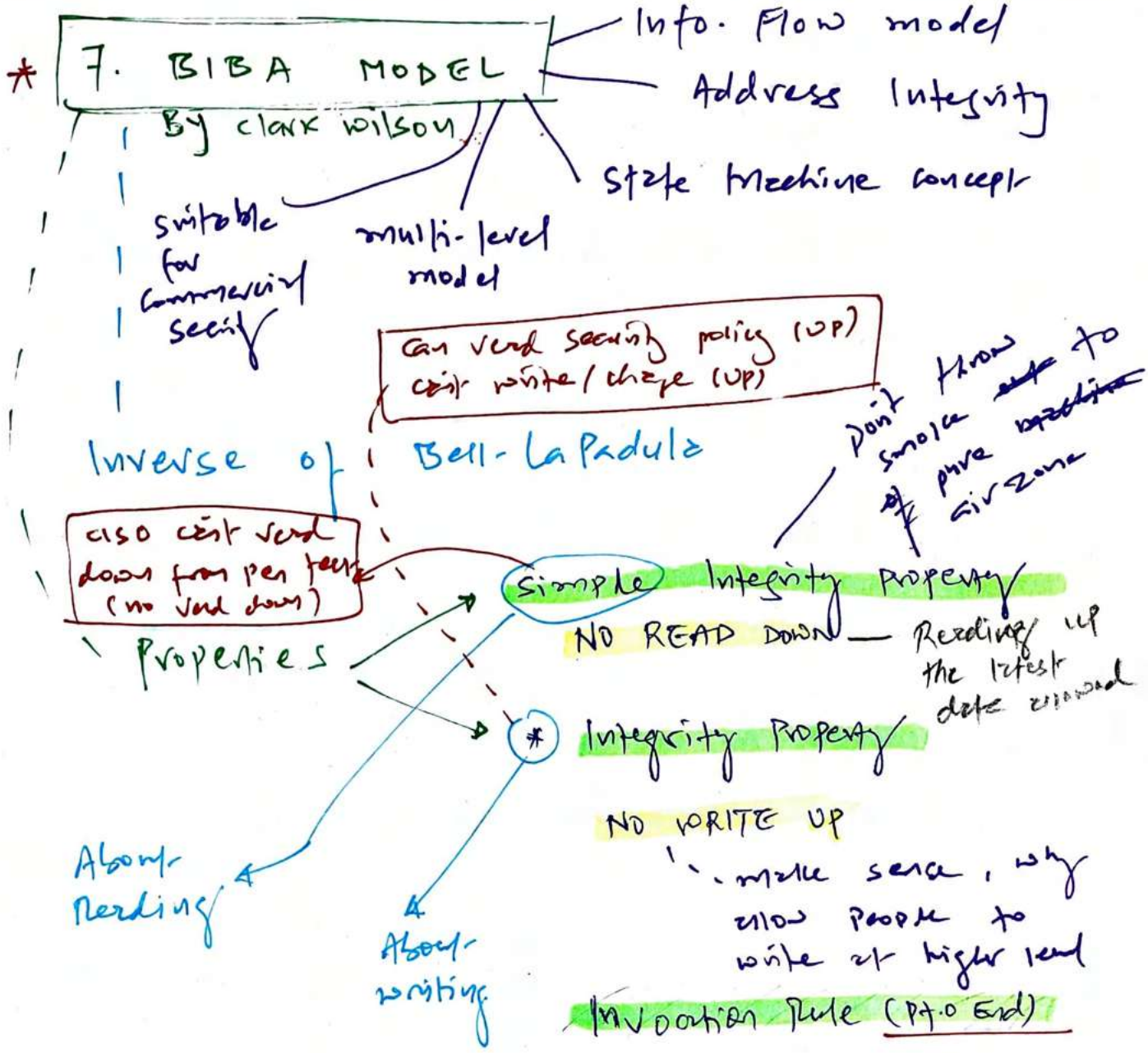
Lattice-Based Access control

- Subjects are assigned with lattice.

- subject can only access objects that fall into range b/w Least upper bound & Highest low bound.



Spy wants to convey message to previous, he can write up



* Biba address three integrity issues:
(3 rules of Integrity)

(1) Prevents unauthorised subjects modifying objects

(2) Prevents authorised subjects modifying unauthorised objects

(3) Protect internal & external object consistency.

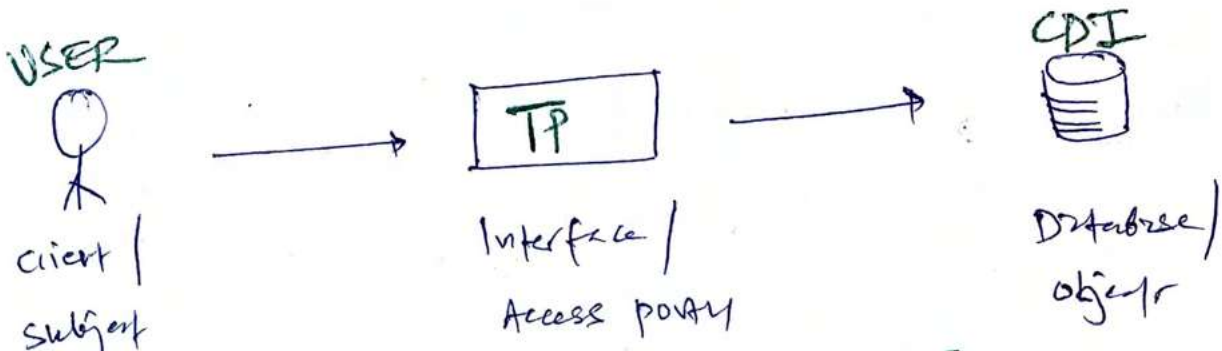
* 6. CLARK-WILSON MODEL — Data Integrity

For commercial Apps.

- No state machine or lattice structure

↓

Instead use three-part-program (triple)



Access-Triple - subject - program - object

(P.T.O End for revised diagram concept)

[Rules] 3 Principles

Enforced Separation of Duties

* Restricted interface model

- Uses security labels as classifications

Well-formed transactions

- Each subject can access object via portal (TP)

- like a program

- Each program has limitations on what it can / it cannot do to object, Hence, limiting subject's capabilities.

- One subject (Confidential)

- separation

- one set of Data + Function

- second subject (Restricted)

- Another set of data + Function

9. BREWER & NASH MODEL

Integrity model

Chinese wall

Dave → Syber → ANZ

Dave ---- Access to proprietary Data ---- Employment

Should not have access to competitor

X Commonwealth

X NAB

X WESTPAC

Principles

other perspective

Data Isolation

- Keeps users (Dave) out of potential conflict of interest

Admin ← Full control

if conflict with Data they

Admin ← Access blocked temporarily only for conflicted data

when resolved

Admin ← Full Access

10. GOGUEN - MESEGUER MODEL.

Integrity

Foundation of Noninterference model

Based on

Automation Theory

- predefined subjects
allows predefined actions
against predefined objects

Domain seperation

- similar subjects grouped = Domain 1

× No access to other domain

11. SUTHERLAND MODEL

Integrity

Based on state machine & Info. flow model

Prevents interference

Integrity maintained through PREDEFINED SECURE STATES & interference is prohibited.

EXAMPLE

Prevents COVERT CHANNEL

OSU Pg 285

- Path / channel normally not used for communication = exploit, violate, bypass security policy

OVERT CHANNEL = Known, Expected, Authorised, Designed, monitored, controlled

12. GRAHAM - DENNIG MODEL

Secure creation & deletion of objects and subjects using eight primary protection rules or action.

SELECT

SELECT CONTROLS BASED ON SYSTEM SECURITY REQUIREMENTS

Buying : 2 step evaluation process

System testing + technical evaluation, meets security capabilities for intended use

Compare system with secure design, individual response, performance

↓

Track changes = ReTest criteria

Management's responsibility to accept RISK when system is approved & Deployed.

3 main product evaluation models

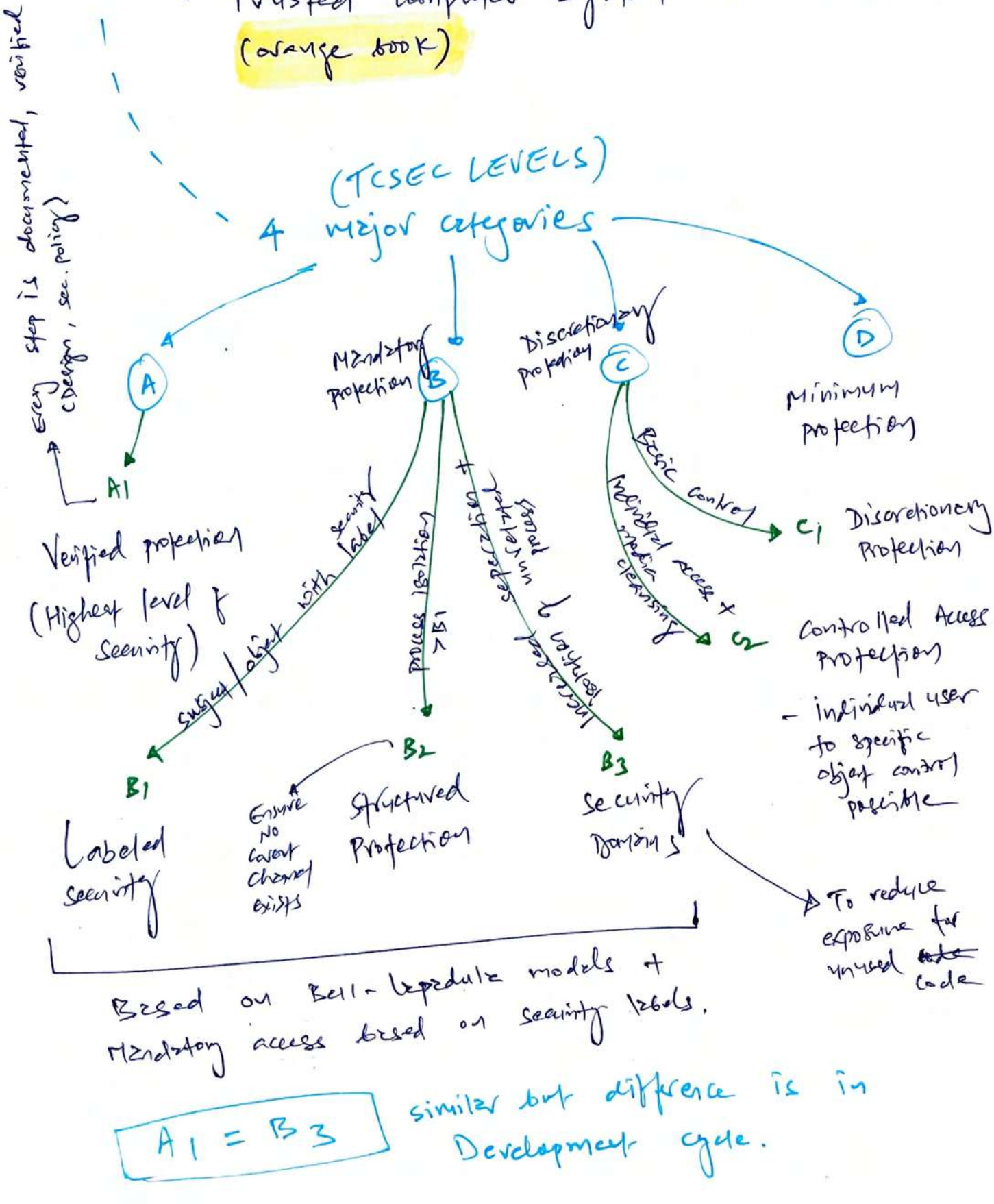
- TCSEC (1980s)
- ITSEC 1990-1998 : European model
- Common Criteria 1998 - replaced TCSEC + ITSEC

2005

1. TCSEC classes & Required Functionality.

TCSEC only Address confidentiality.

Trusted computer System Evaluation Criteria (orange book)



A1 = B3 similar but difference is in Development cycle.

* Rainbow series

Orange book : Applies to stand-alone computers, not attached to a network.

Red book : Interprets TCSEC in networking context

Green Book : Provides password creation & management guidelines.

* Problems with TCSEC → Replaced with common criteria in 2005

- Focus on C, Not I
- Doesn't address personal, physical & procedural policy to implement full security policy.

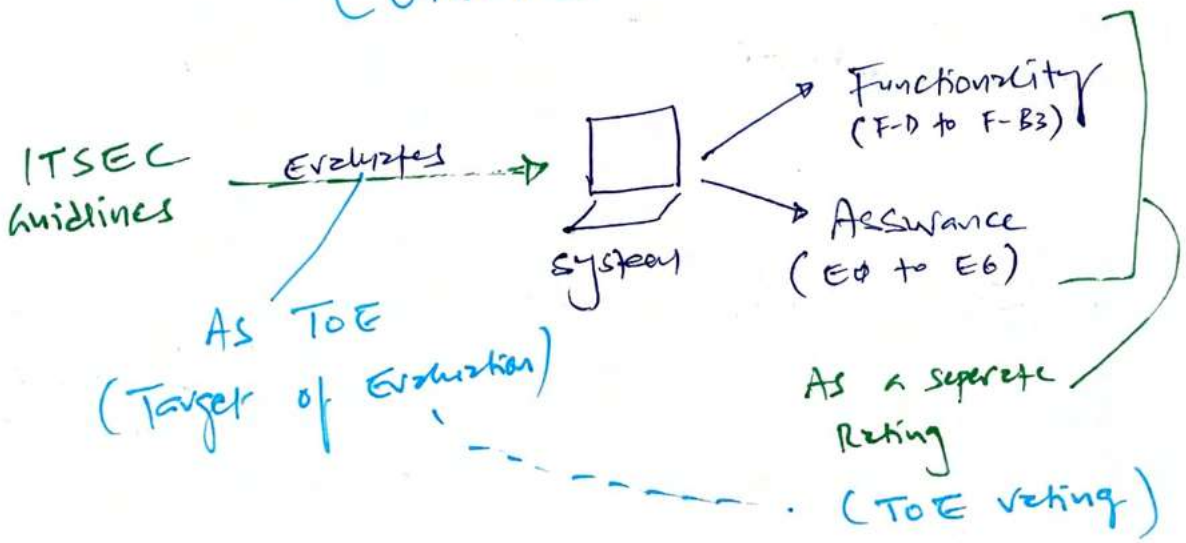
side notes, not bad.

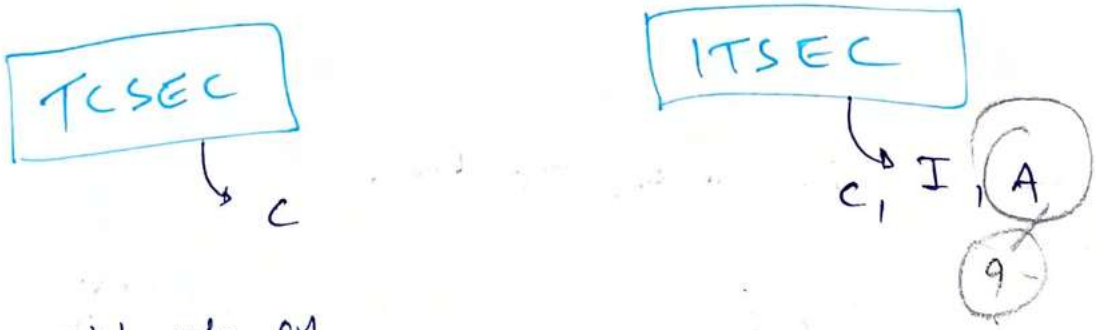
TCSEC	Common Criteria (CC)
- Address only confidentiality	- Address CIA
- US Domestic	- International
- NCSC scope	- Broader Scope
- Rigid model	- Allows flexibility
-	

2. ITSEC classes & Required Assurance & Functionality.

Information Technology Security Evaluation Criteria

- Initiated for evaluating Security criteria in EUROPE





- Doesn't rely on TCB (system components doesn't need to isolate within TCB)
- changed system requires to be Reevaluated → doesn't need it.

FIRST PTO for 10,000 feet AT END

3. COMMON CRITERIA (CC)

Helps customer buy with confidence

→ Designed as a PRODUCT EVALUATION MODEL

> High CC rating ≠ secure system, free from VULS.

→ official standard: ISO 15408
(Evaluation criteria for Info. tech. security)

- CC process based on two elements:

Protection Profiles (PP)

- For product evaluation that meets security requirements & protections

↓

SECURITY DESIRE
("I want" from customer)

Security Targets (ST)

- Implemented security measure from vendor built into target of evaluation (TOE)

↓

"It will provided" from vendor for specific system such as Cisco ASA

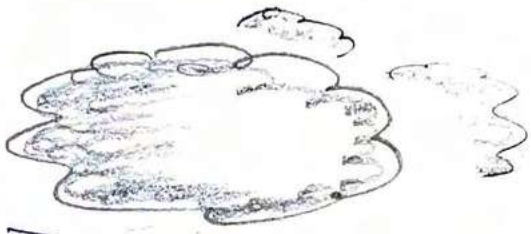
Customer PP ↔ ST Vendor 1 (TOE)
Customer PP ↔ ST Vendor 2 (TOE)
Customer PP ↔ ST Vendor 3 (TOE)

↓

closest / best match is client purchase

* Cloud-Based Systems and Cloud computing

PCIDSS → Answer
HIPPA
FISMA



Cloud is good but

- Privacy concerns
- Compliance difficulties (Regulations) (Jurisdiction)
- Lost privacy control
- Is data secured there?
- Standards
- Inconsistent security policy b/w cloud provider & organization

[Hypervisor
(VMM - virtual machine monitor)

→ create, manage & operate virtual machines

Type I Hypervisor (Runs on BARE METAL Native)

- No host OS
- Hypervisor directly installs onto hardware where host OS reside
- used to support Server virtualization
- most efficient as it requires no OS loading
- highly secure as it eliminate OS vulnerabilities

max. utilization H/W, reduction of risk by host OS

Type II Hypervisor – Runs on top of OS

- Regular H/W OS + hypervisor instal another S/W app.
- Used for Desktop deployment (Guest OS, Sandboxing)
- cheaper than type I but not secure

Cloud storage
- cost effective backup but not high speed
- ? Is data secured?

Elasticity — Flexibility of virtualization resources on demand

Autoscale

Cloud concepts

CASB — DLP
(typically not responsible if you leak confidential info. Use below solns.)

PaaS
- AWS Elastic Beanstalk
- Azure

H/W & S/W tools available on Internet
- looks after infra, physical security, maintenance but you have to worry about software & code

SaaS
- Google Drive
- MS 365

S/W by 3rd party on Internet

IaaS
- AWS EC2
- Google Compute Engine (GCE)

Cloud-based service, pay-as-you-go for storage, networking, virtualization

Deployment concepts

Hosted Solution

Organization own its license S/W, then operate + maintain the S/W

Cloud Solution

Organization outsource H/W + S/W to 3rd party cloud provider for monthly fee.

- Private cloud
  - Virtual private cloud
- Public cloud
- Hybrid cloud
- Community cloud
  - shared benefit + collaborative work

Investigate Security of cloud provider

- Compliant?
  - PCI DSS
  - HIPPA
  - SOX
- How they do Disaster Recovery?
- Review patch management policy
- How they respond to zero-day attacks?
- Review their Data Encryption solutions
  - How Data is backed up?
  - How they destroy data?
- How they provide availability of resources?
- How often they perform Pentesting?

Is CASB Implemented!

(Cloud Access security Broker)

- To enforce Proper security measures are implemented or not.

Security as a Service (SECaaS)

- cloud provider concept
- From managing security locally to online = reduce cost + overhead

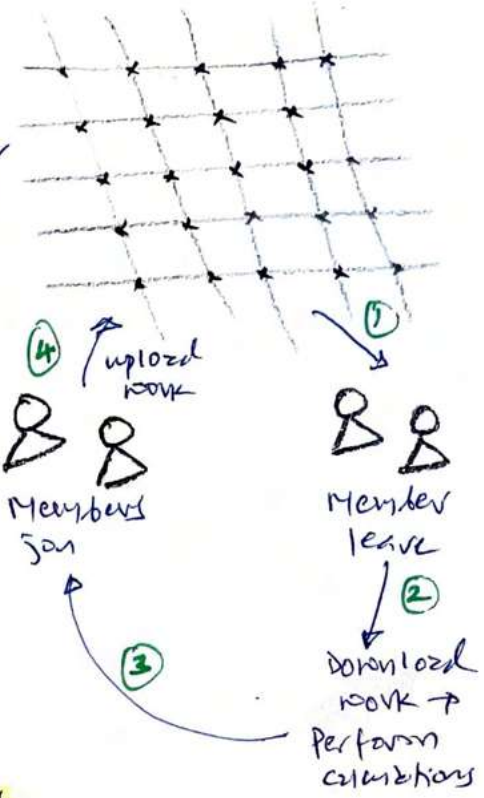
Cloud shared Responsibility Model

Who will do?

- Security
- Troubleshooting
- management

* Grid Computing

- Form of parallel distributed processing that loosely groups a significant number of processing nodes to work towards a specific processing goal.



Security concerns

- Contents are exposed to the world = no confidentiality / privacy of data
- Compromise of grid server = leverage grid members to perform malicious actions.

* Peer to Peer (P2P) - TORRENT

Networking & distributed application solution that share tasks & workloads among peers.

Similar to grid computing with 2 differences

- No central management system
- Provided Services = Realtime Not collection of computing power

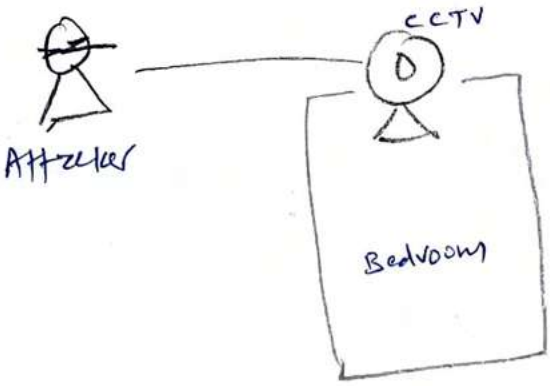
Security concerns

- Eavesdrop distributed content
- Pirated copyrighted materials
- No control mgmt / filtering
- Can consume all available bandwidth

INTERNET OF THINGS (IoT)

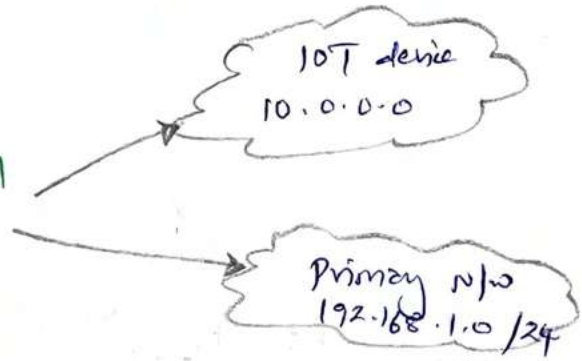
Security concerns ---- NIST Initiative for IoT

- Access
- Encryption



isolate IoTs into seperate network

Secure Implementation for IoT (THREE DUMB ROUTERS)



INDUSTRIAL CONTROL SYSTEM (ICS)

- ICS controls industrial processes and machines.

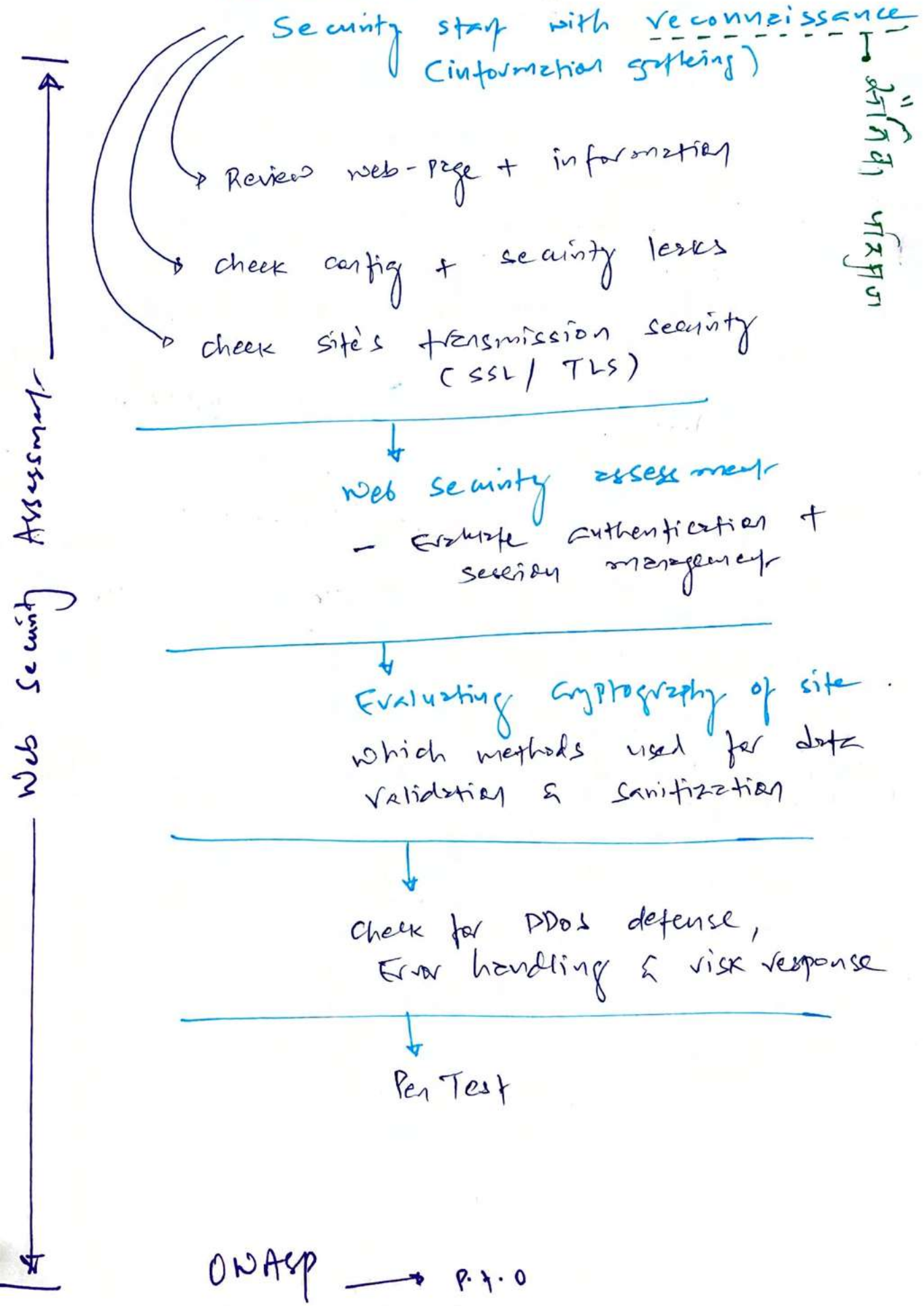
3 forms

- Distributed control system (DCS)
- Programmable Logic Controller (PLC)
- Supervisory control and Data Acquisition (SCADA)

Needs less Human interaction = little security was Built

Until Stuxnet delivered virus kill in SCADA

ASSESS AND MITIGATE VULNERABILITIES IN WEB-BASED SYSTEMS



Few of OWASPS Top 10 Web Risks

INJECTIONS

SQL Injection

Use of unexpected / malicious code as query to compromise web application / database.

↓

static to dynamic web page story on How did we reach here.

2 techniques

- Input Validation
  - type + Format & length of input
  - E.g six numeric for DoB
  - 230283
- Limit account Privilege
  - least privilege

LDAP Injection

Focus on LDAP directory, not database

XML injection

Backend target is XML Application

- Sanitizing of input & defensive coding as prevention

XML Exploitation

- Programming attack either use false information to visitor or cause system to give-up information without authorization.

↓

SAML abuse = web-based authentication

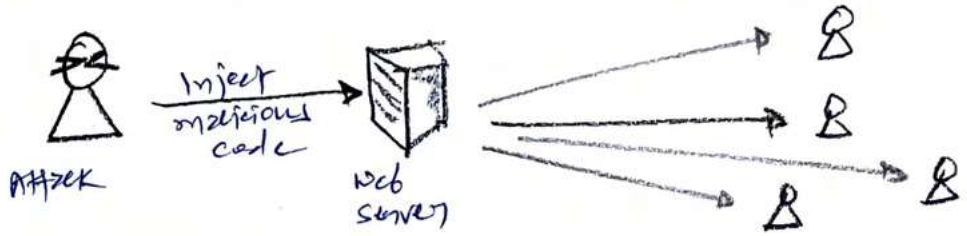
Used for web SSO solution

Attacker can falsify SAML communication or steal visitor's access token, to bypass authentication & gain unauthorised access to site.

SAML = XML use

Cross-site Scripting (XSS)

- Malicious-code injection attack



- Defense → WAF
  - Patched web server
  - HIDS
  - Input validation
  - metacharacter filtering.
  - Avoid malicious / non-mainstream websites
  - Run Antivirus s/w

Cross-site Request Forgery (XSRF)

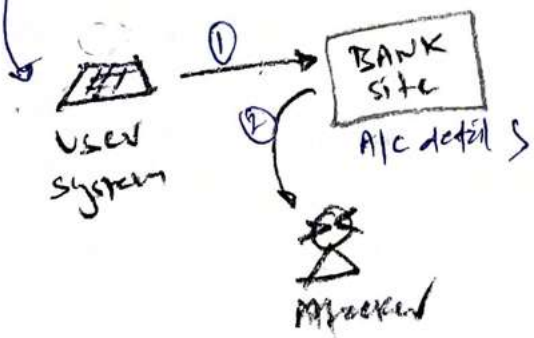
- Attacker Focus = visiting user's web browser, not visiting website

Purpose

To make user / user's browser to perform unattended action
- Make a purchase
- Download A/c details
- change A/c information

XSRF

Eg: ZEUS



Defense

- Sensitive action = Reauthenticate (Netcode)
- CAPTCHA → Human / machine
- Nonce: Add random string to each URL + session mgmt
- WAF, HIDS
- Patch browser, clear cookie + temp Internet files.