13. MANAGING IDENTITY & AUTHENTICATION

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

PERSPECTIVE

Types of Access controls
- Preventive
- Detective
- Corrective

implemented As
- Administrative
- Logical (Technical)
- Physical

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

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

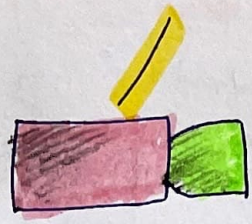
Authentication Factors
Type - I, II, III

AAA Protocols
- RADIUS
- TACACS
- Diameter

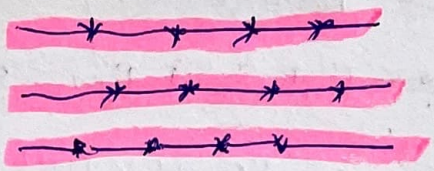
IAM Lifecycle
- Provisioning
- Account Review
- Account Revocation

* Types of Access control

Preventive Access Controls



CCTV



Fence

IPS + Firewalls

Antivirus software

Security policies

Security awareness & Training

Detective Access controls

motion detectors

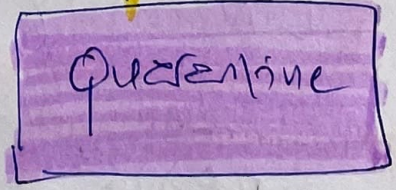
Security Guard

Job Rotation + Mandatory vacation

IDS + Honeypots

Corrective Access controls

Virus



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

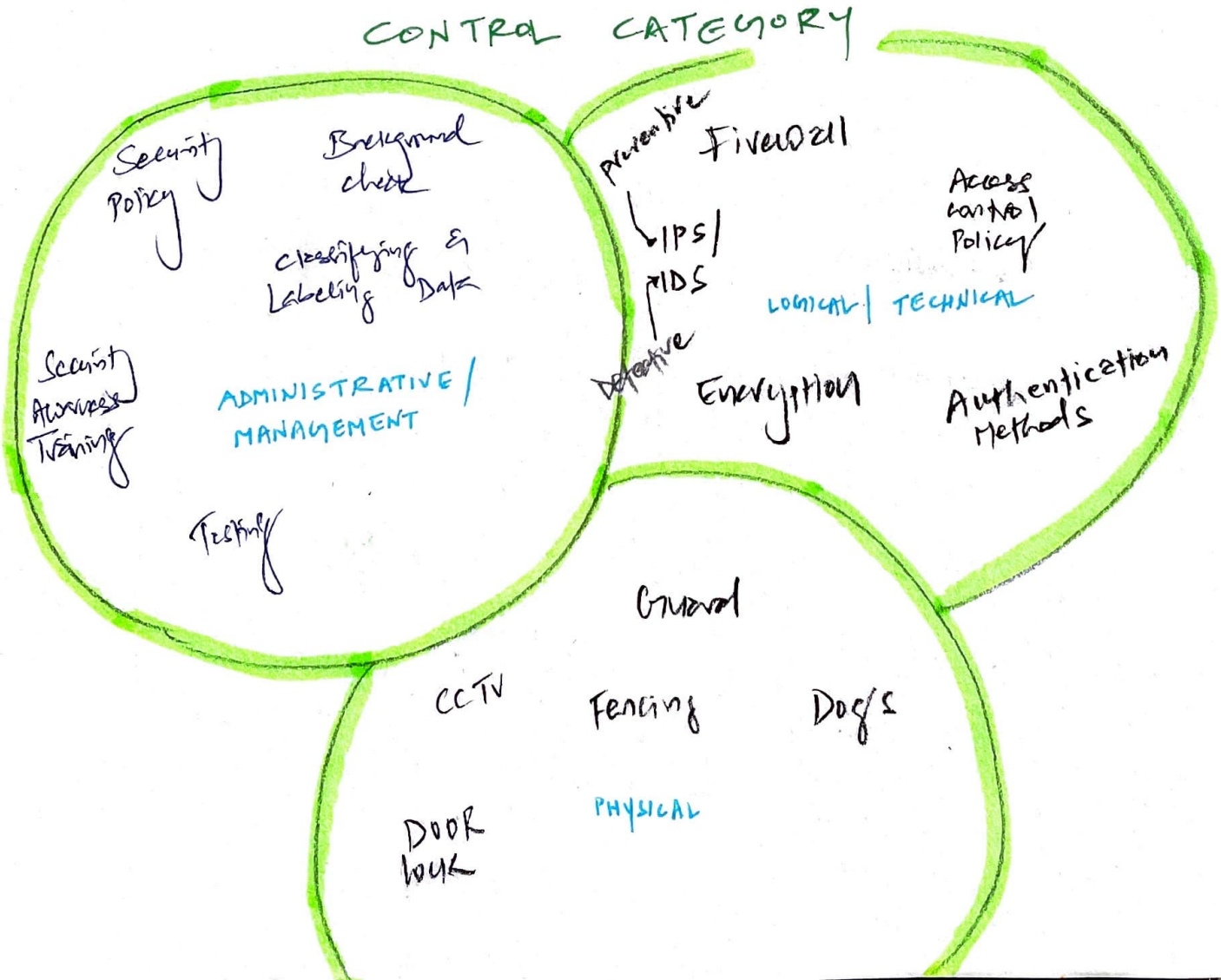
* other controls

Deterrent → Discourage → signboard / warnings

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

Directive → Enforce security policy (compliance) | DETOUR SIGN

Compensating → Alternate



Effective identification + Authentication
+ Auditing

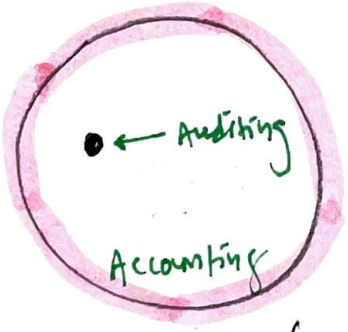
⇓

ACCOUNTABILITY

No Authorization

Identification
+
Authentication

→ Authorization → Accounting



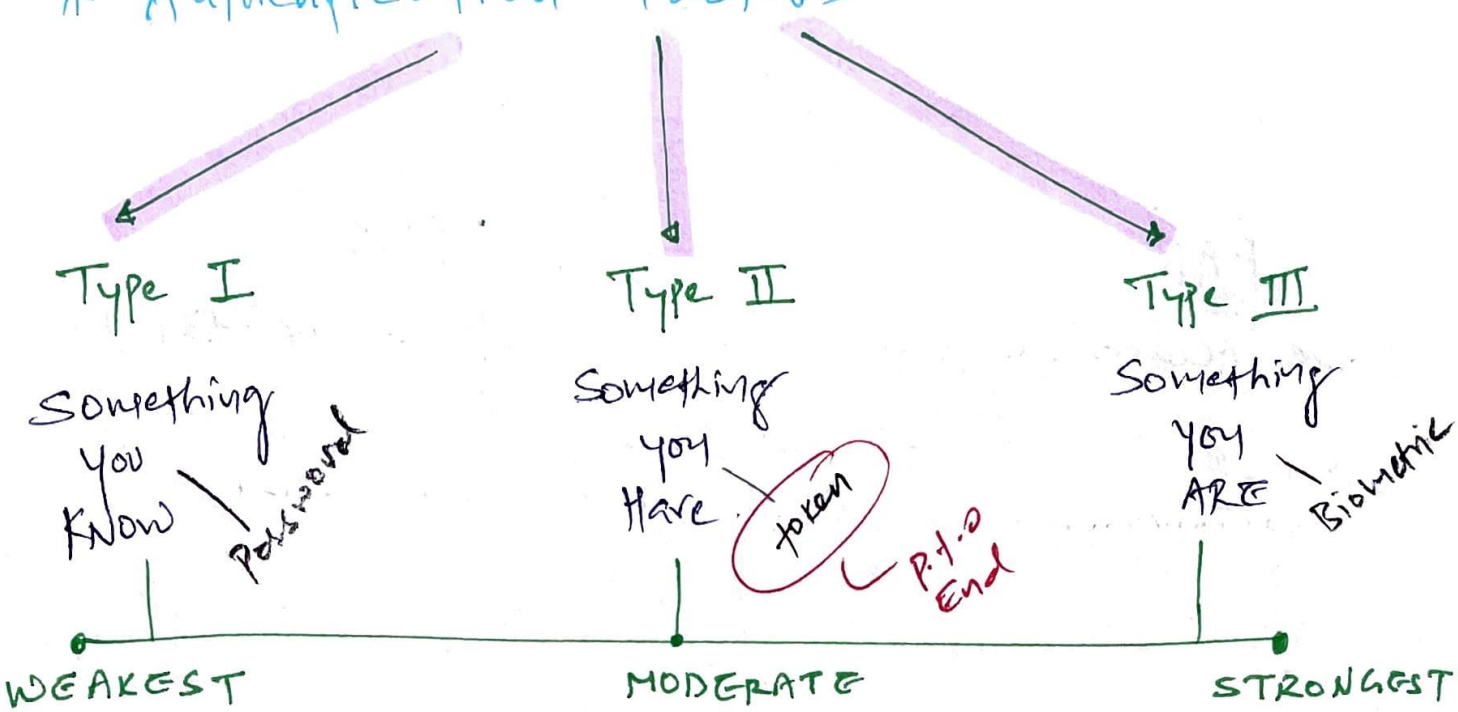
Logging user actions based on their proven identities provides

Logging + Monitoring
+ Auditing

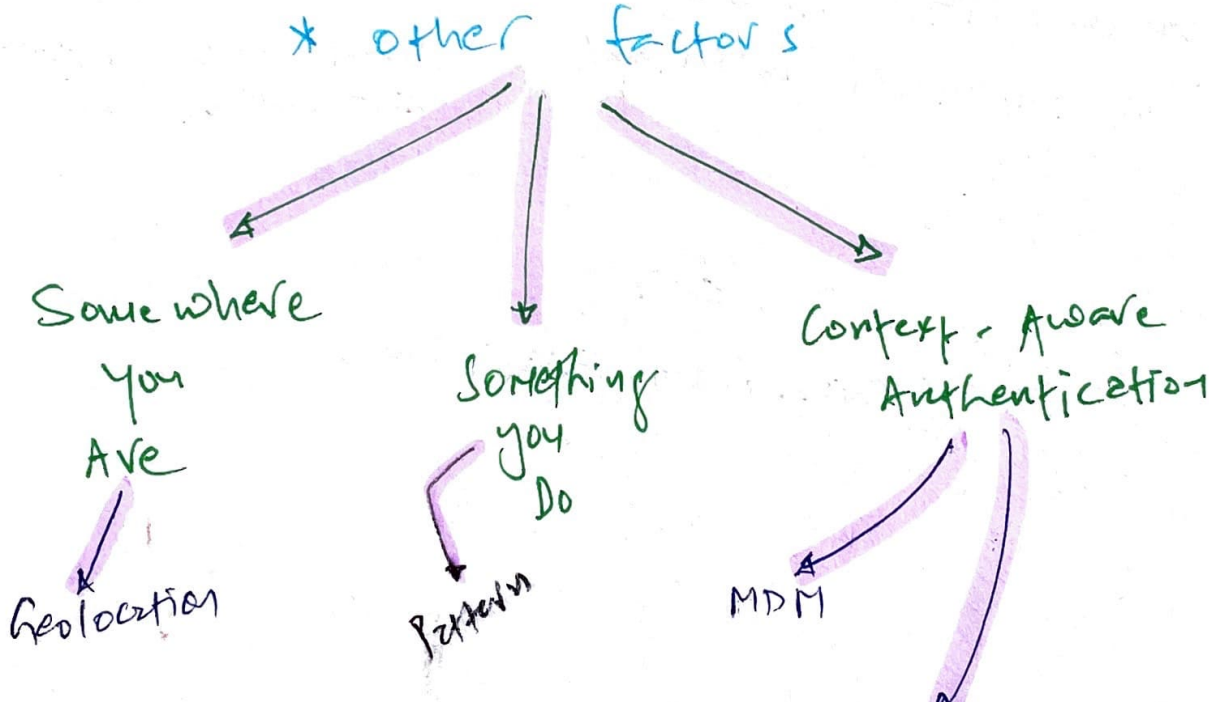
⇓

ACCOUNTABILITY

* Authentication Factors



* other factors



Two-step Authentication

- HOTP
  - Hash-based one time password - value remains till used
  - Network Code
- TOTP - Time OTP - code expires such as 30-seconds

NOTE - what if OTP displayed on mobile as pop-up notification. How is that secure.

Check NIST 800-63B

Biometrics

Type 2 Error

FAR

(False Acceptance Rate)

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

or false positive is when invalid subject is authenticated

Type I Error

FRR

(False Rejection Rate)

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

or false negative is when valid subject is not authenticated

CER

(Crossover Error Rate)

- To determine the quality of Biometric system

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

Biometric Device Sensitivity

High
- FRR increases
- More false negatives

low
- FAR increases
- More False positives

↑ FRR → Prim for support

↑ FAR → Not good for security

Methods for Device Authentication

- 802.1X
- MDM + NAC
- External IdP

* IAM Implementation

- SSO
- Kerberos — p.t.o
- LDAP & PKI
- Federation Identity Mgmt & SSO

Passwords

- Static — same length password (workers) — 30/60 days
- Cognitive — those stupid security Questions
- Dynamic — one time use password changed at every 60 seconds
  - e.g. OTP

Password Storage

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

Provides "C" + "I"

KERBEROS

→ Primary purpose = Authentication

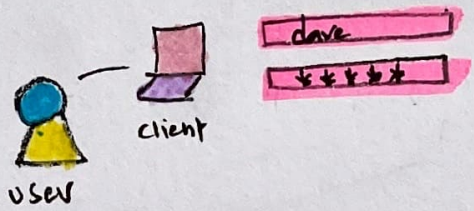
— deserves a video

↳ For SSO

P.T.O End for diagram

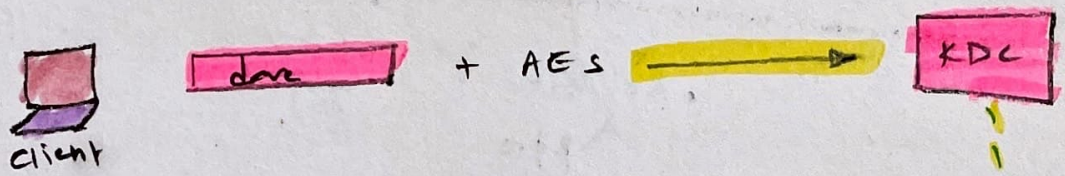
kerberos logon process

1



User types username & password into the client

2

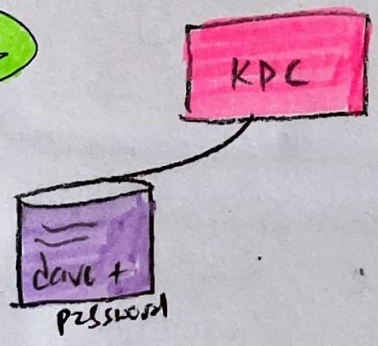


client encrypts the username with AES & send to KDC

All clients & servers are maintained in KDC

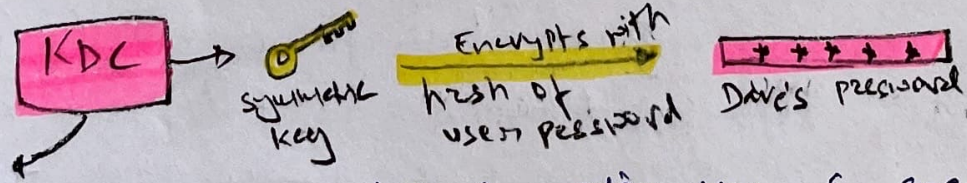
Key distribution centre - trusted 3rd party that provides authentication service using symmetric cryptography

3



KDC verifies username against database of known credentials

4



TGT

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

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

6. client installs TGT for use until expires.

client decrypts symmetric key with user's password.

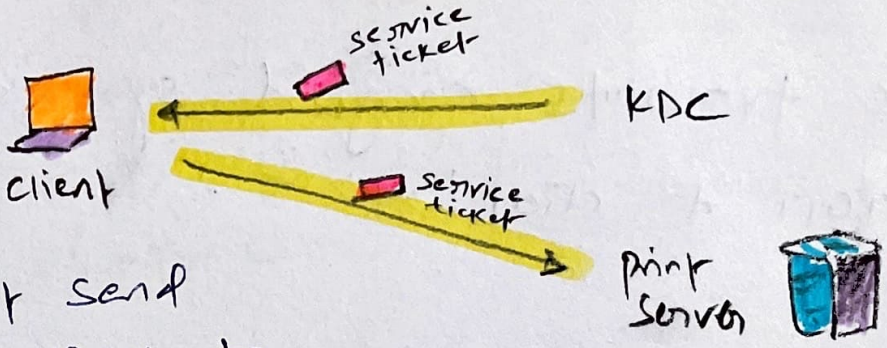
Note - Security is user password is never transmitted - the symmetric key will ~~encrypt &~~ decrypt if user know ~~the password~~

when client want to access object

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

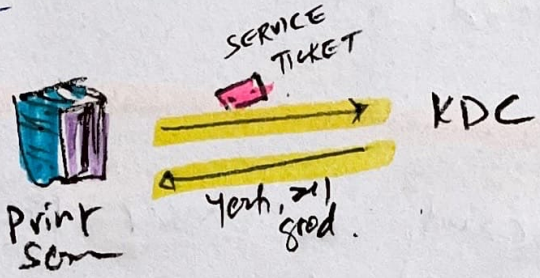
KDC generates service ticket & send to client.

4



client send service ticket to print server

5 Server verifies the validity of ticket with KDC



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

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

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

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

AAA Protocols

RADIUS ← Not for SSO

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

(improvements)

Diameter

- TCP port 3868
- Supports IPSec & TLS

TACACS

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

RADIUS → Centralizes authentication for remote connections

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

Diameter → supports traditional IP, mobile IP, VoIP

Federated Identity Manager & SSO

End of P.t.O

Revised concepts from All-in-one

A common language to communicate with different federation organizations.

SAML — Security Assertion Markup Language

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

SPML — Service provisioning Markup language

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

XACML — Extensible Access control Markup Language.

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

OAuth 2.0 — Open Authorization

- Sign-up to canva using Twitter credentials.

P.t.O

OpenID — Decentralized Authentication

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

OpenID Connect — Authentication layer using OAuth 2.0 framework

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

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

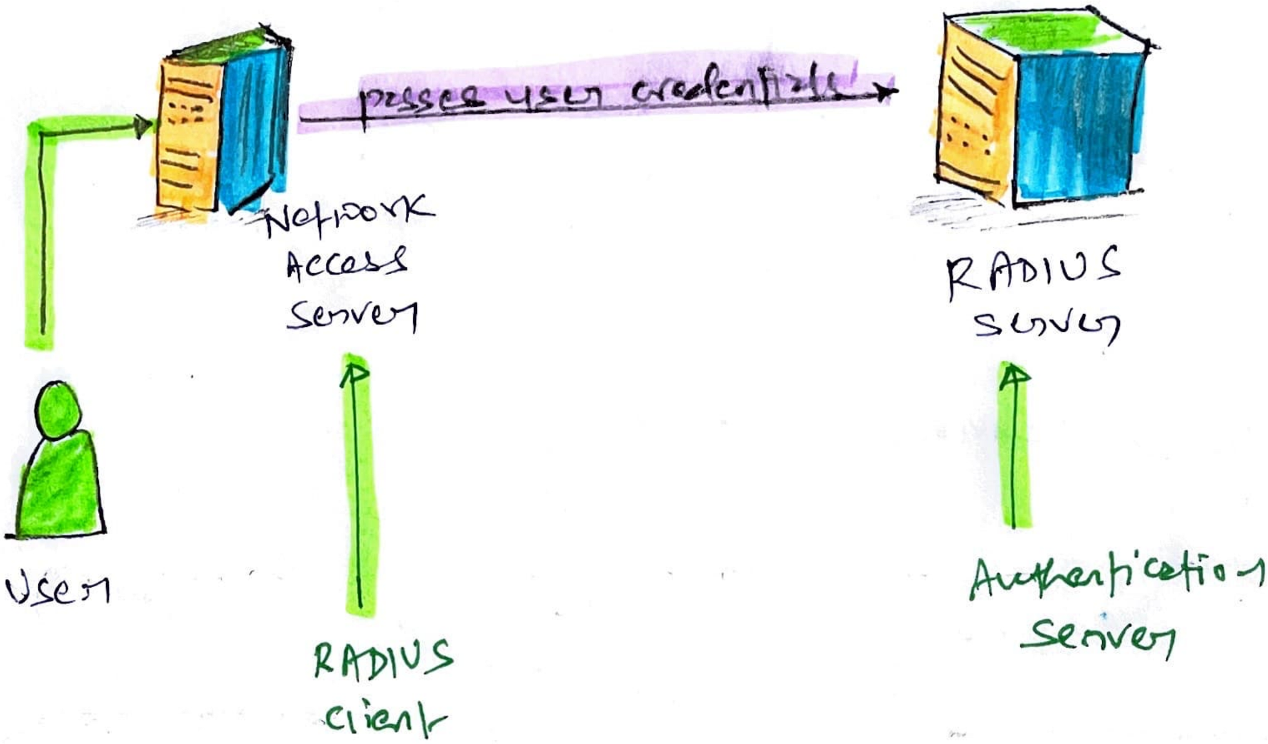
OAuth — Allows access to resources from another service

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

Kerberos + LDAP — for in-house services

LDAP — P.T.O — End xx

RADIUS Architecture



Kerberos
ADFS
Central Authentication Service (CAS)
] ✓ SSO

RADIUS × SSO

p.f.i.o summing

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

Tokens

Synchronous Dynamic Password Tokens

time based passwords that expires in 30/60 seconds.

Asynchronous Dynamic Password Tokens

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

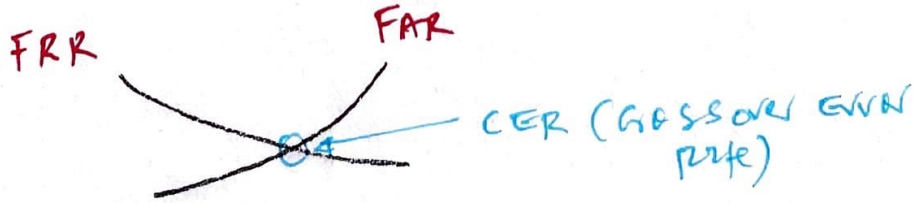
Biometric Ultimate summary

Type I — FRR — False Rejection Rate

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

Type II — FAR — False Acceptance Rate

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



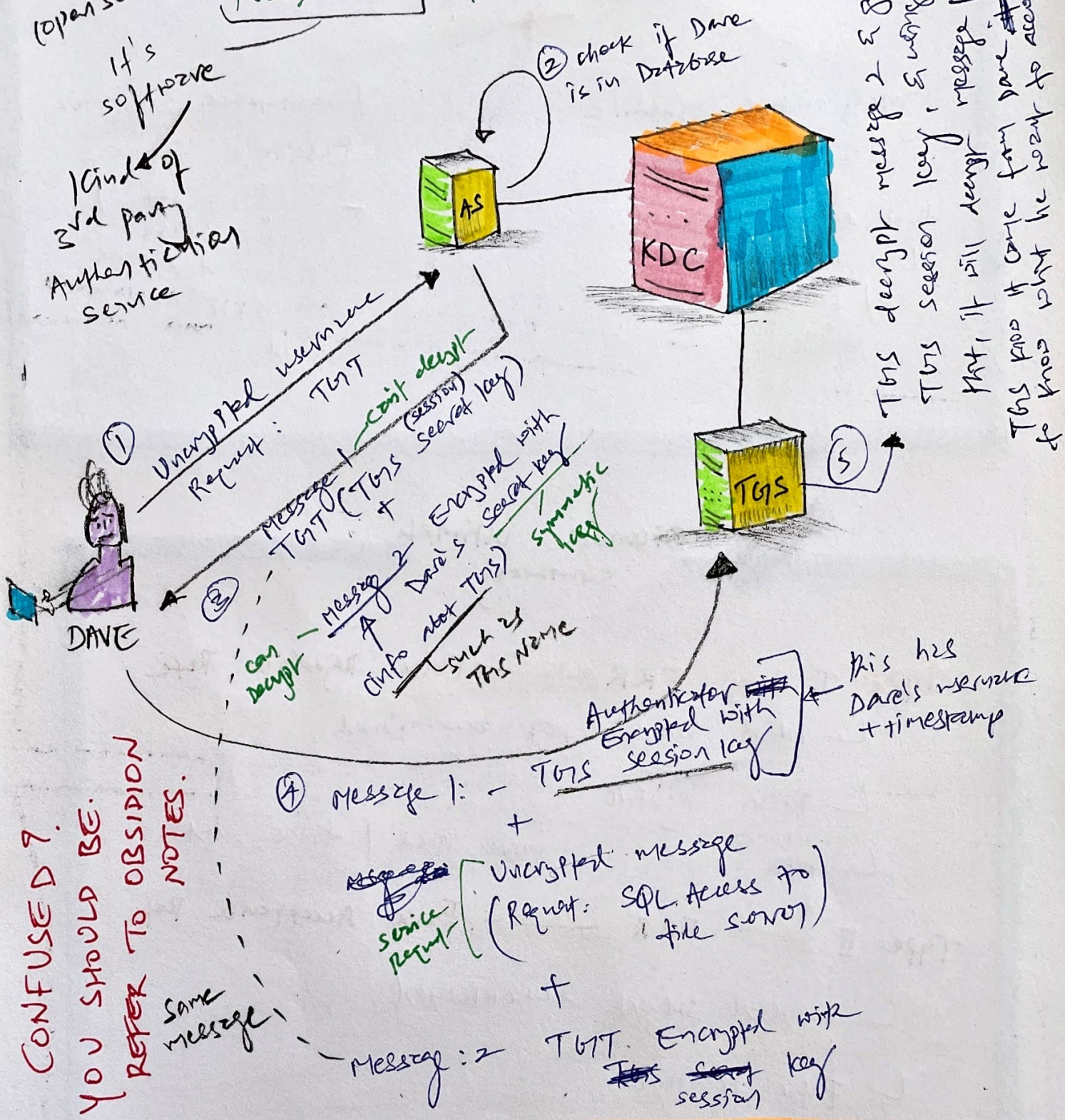
- low CER = Accurate Biometric System
- False Negative is better than False positive

Kerberos, From Luke A.

(open source)

It's software

Kind of 3rd party Authentication service



CONFUSED?
YOU SHOULD BE.
REFER TO OBSIDION NOTES.

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

Perspective

KDC

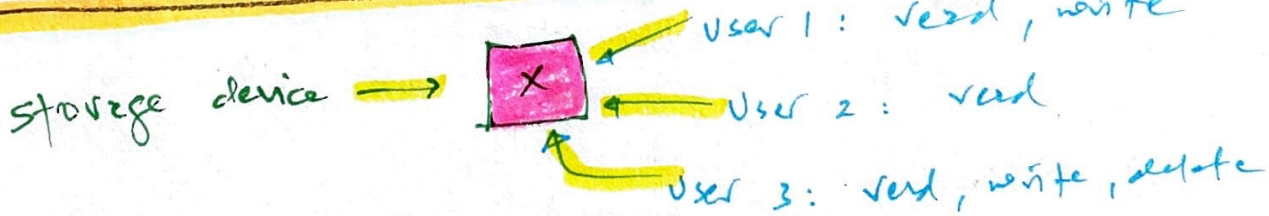
- KDC vouches for individual's identities using tickets.

CA

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

Attacks

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



what type of Access control is used?

↳ Resource-based Access control → Matches permission to resource like a storage volume. They are common in cloud-based infra.

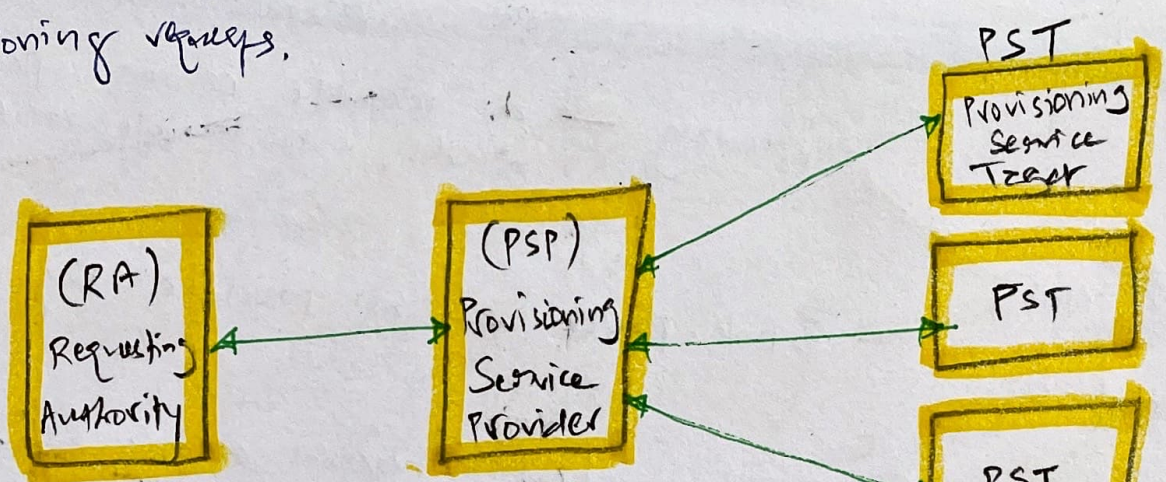
~~X~~ RBAC
~~X~~ MAC
~~X~~ RUBAC

SPML - Service Provisioning Markup Language

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

↓

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



SPML client

Initiates a/c request for new employee

SPML server

Review request & compare with organization's accepted criteria

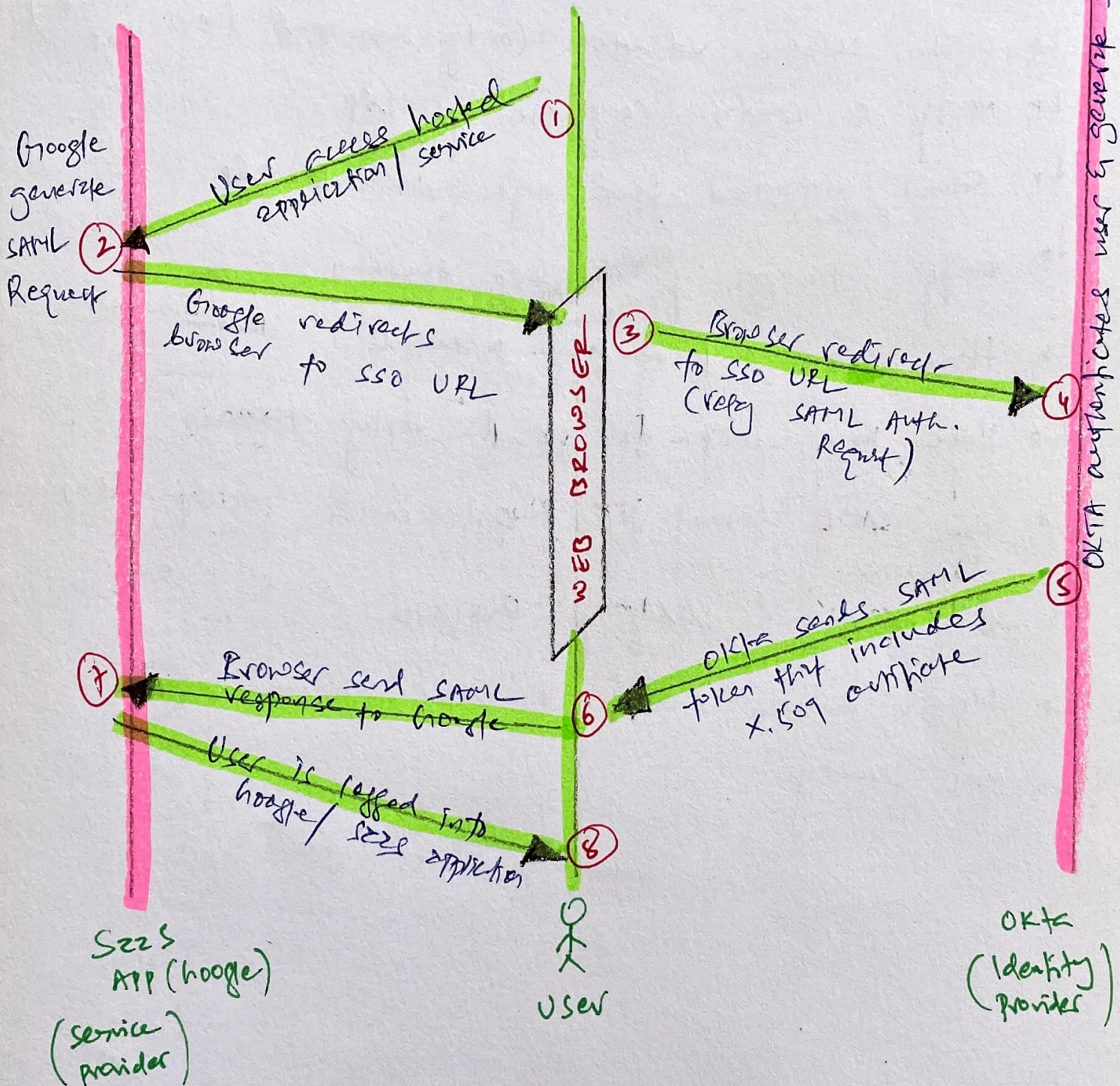
Target Systems

Setup necessary a/c & configurations for access rights

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

SAML - Security Assertion Markup Language

(security concerns - P.t.o)



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

Note - SP & IDP already established trust using PKI (X.509) befor SAML.

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

* SAML Security Concerns / Precautions

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

LDAP

→ LDAP is part of AD — LDAP is protocol that allows users to query AD and authenticate access to it.

Light-weight Directory Access Protocol

Microsoft AD is LDAP Based like Telephone Directory.

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

LDAP is centralized Access control system + supports SSO.

Note - Simple Authentication & Security layer (SASL) is secure ~~one~~ Authentication mode for LDAP.

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

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

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

Global catalog services — uses port 3268 & 3269