to ensure accountability

Authentication → Non-Repudiation is there

→ Digital Signature → uses public key encryption → when we trust 3rd party → Huge cost

→ MAC → Uses shared symmetric key → Low cost

↓ No dependency on 3rd party

Integrity

(increasing order of work)

→ ~~HASH~~ → simple integrity.

→ MAC → Integrity & Auth.

→ Dig Sign → int, Auth & Non-Repudiation

DC+1

Confidentiality.

Cost ↑

→ Public key Encryption → req. 3rd party. → when no. of users are huge → Key exchange method.

→ Symmetric key Enc. Encryption.

11th Oct 2023

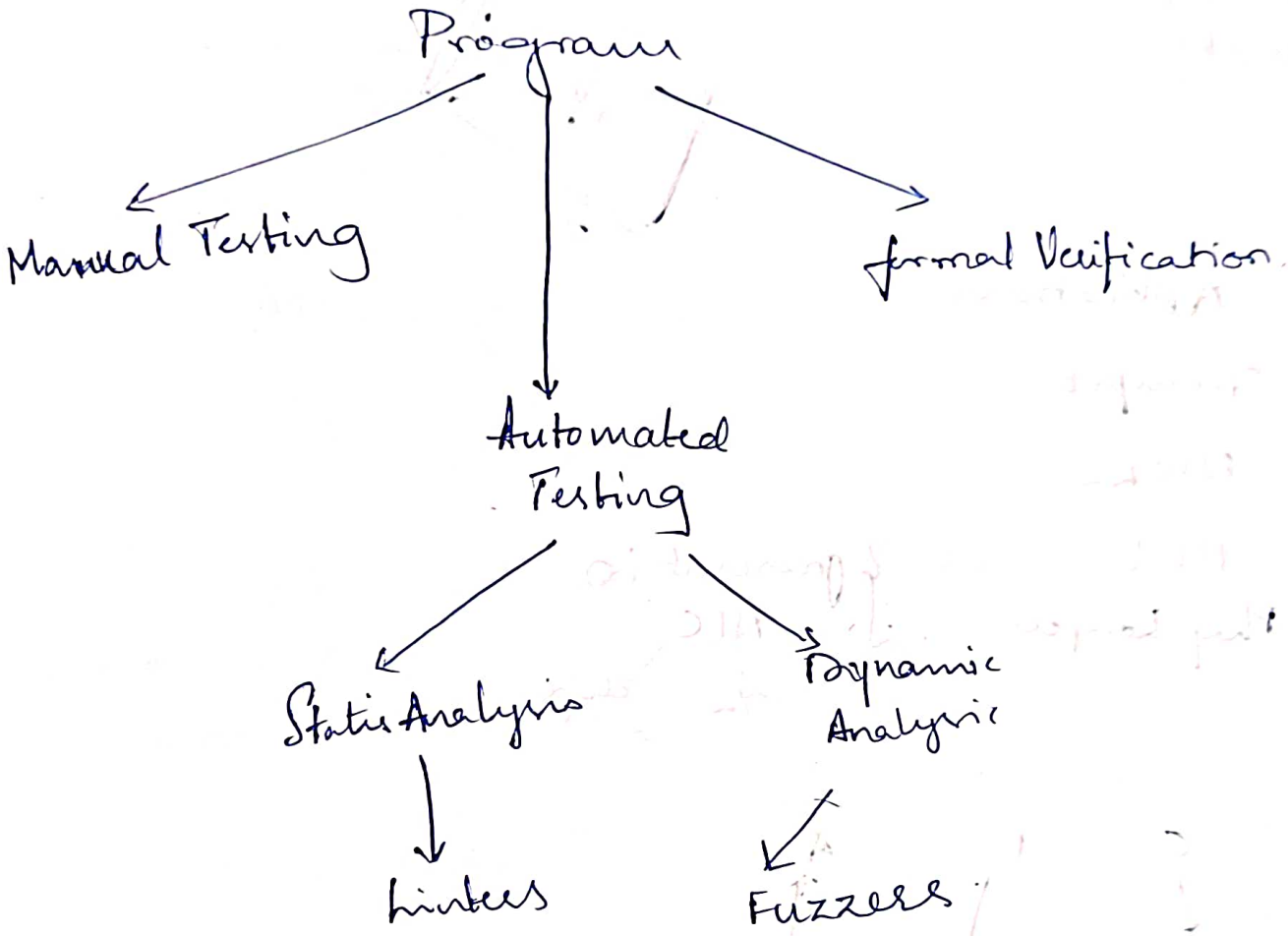
→ Risk Analysis

Cost of Risk Analysis < Loss

Network Security

11th Oct 2023

- Static Analysis
- Dynamic



Rice Theorem:

Network Security :

design issues are dealt here.

zero day attacks

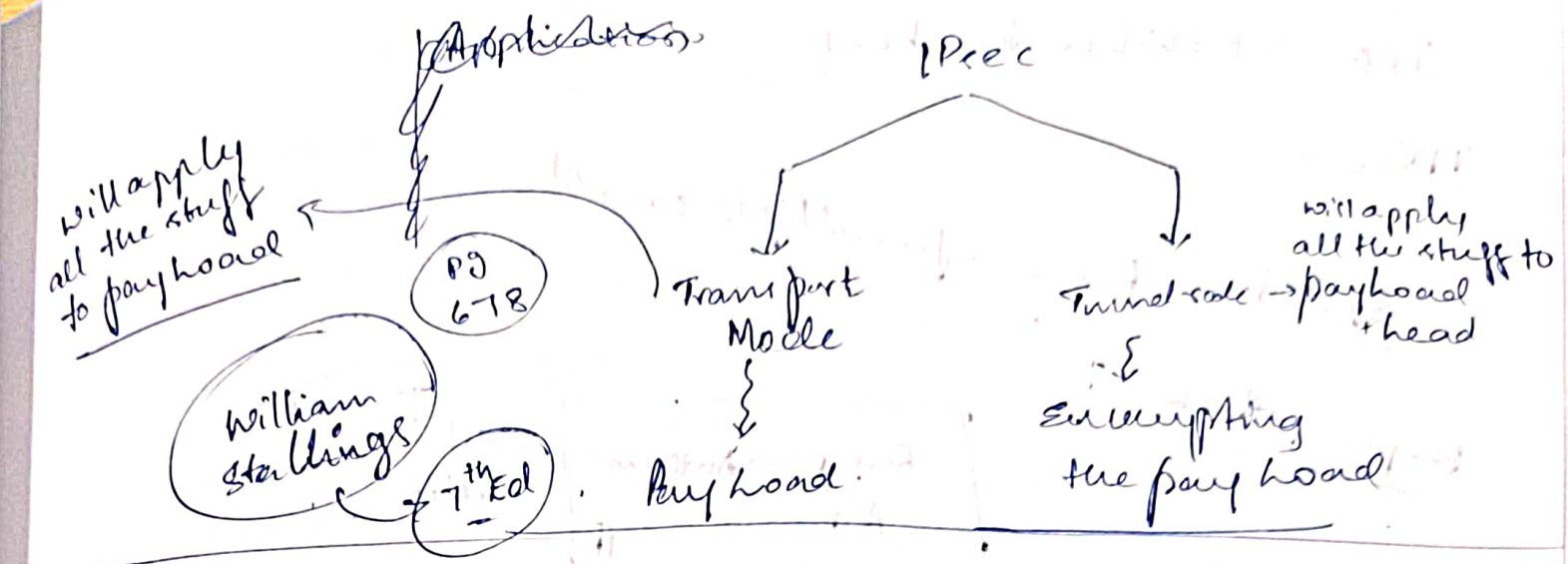
- Application
- Transport
- NW L
- DLL
- Phy Layer

} present in NIC → H/w → chip

C → Encryption → Symmetric key.

I → Hash

A → MAC



13th Oct 2023

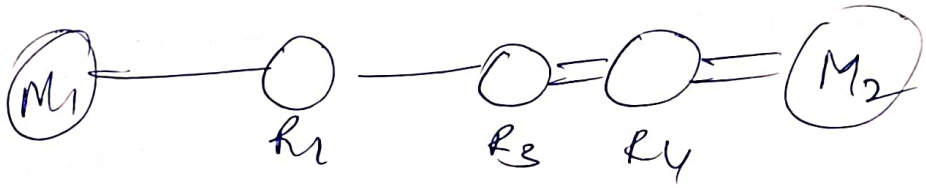
Tunnel ⇏ Not used for end-to-end.

⇓

Used for Routers / Gateway.

IPsec can't be implimented b/w sender & receiver, it can only be applied to sender ~~post office~~ router & receiver ~~post office~~ router.

Can we do this b/w Machines?



IKE : Establishes the key

IPSec :

Spi Numbers → for multiple comm

Replay attack

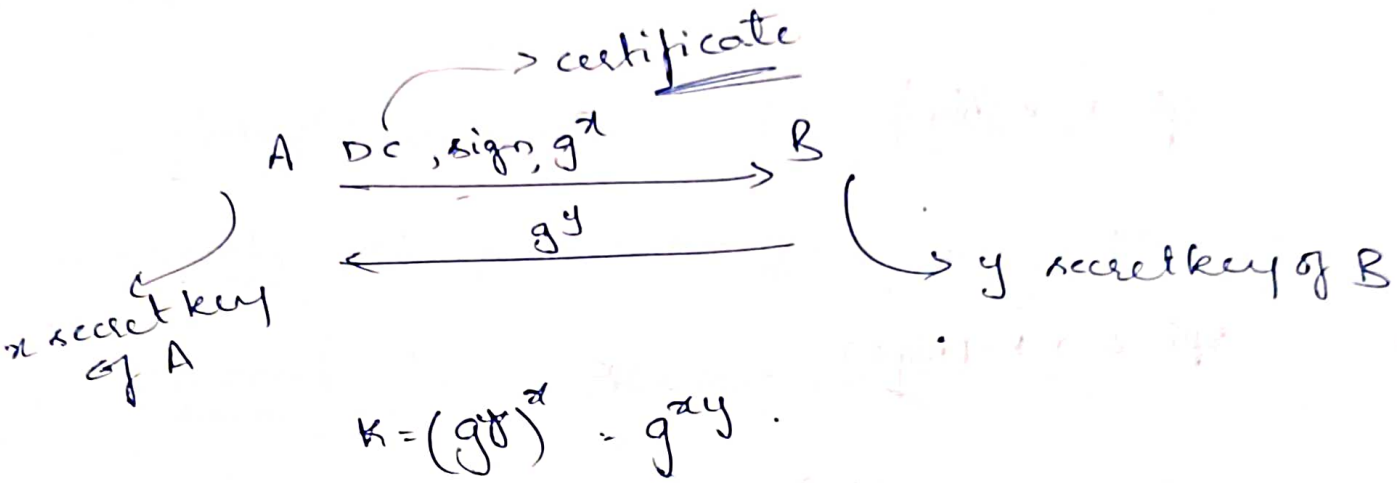
Encryp → Authen Authen → Encryp

which is better ?

Task: to achieve CIA

16th Oct 2023

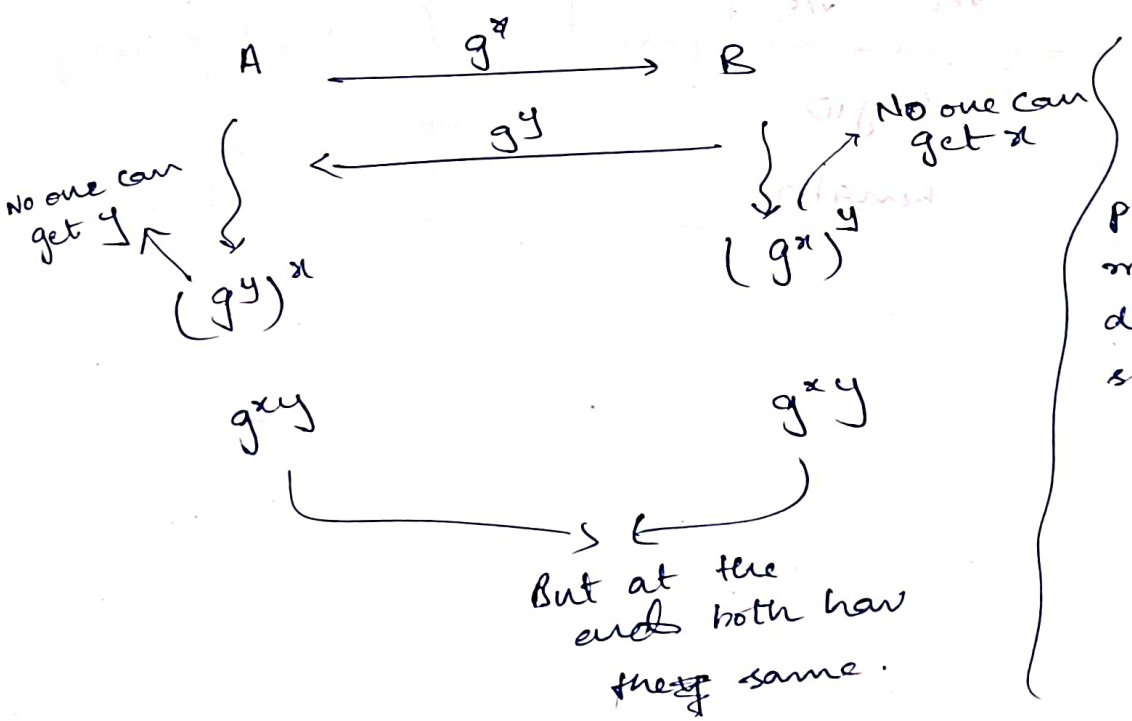
IKE Protocol → used for key establishment



$y = g^x$, if you know 'y' and 'g' then you can't compute 'x' in polynomial time.

"Discrete Log of Assumption"

i.e y → public
g → "
x → secret ⇒ No one can hack in polynomial time.



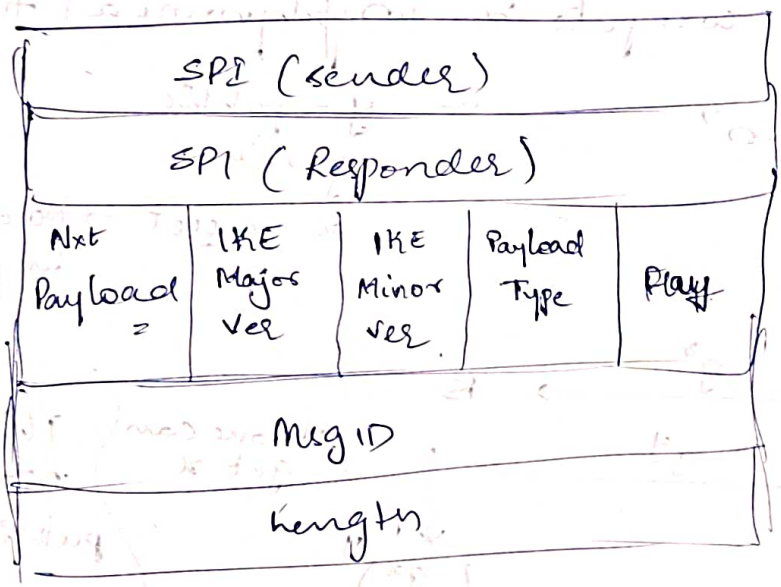
This is the reason why public key takes more time to decrypt than symmetric key.

→ first the receiver verifies the Digital Signature and then process the key $(g^x | g^y)$

spi = 1, K = (Algo) B

A spi = 2, K = (Algo) C

spi = 3, K = (Algo) D



Transport layer Security

18th Oct, 2023

20th Oct, 2023

Protocol stack :

Record protocol : Encryption / Authentication

Handshake : What protocols & stuff.

(proton mail)

Alert protocol : Pointing the errors out.

↳ This isn't there in N/w Layer cause it has ICMP

SMIE attack. SMTP.

↳ done at individual level.

23rd Oct, 2023

DKIM → Authenticates for Domain identification.

(TLS)

Spoofing attack.

PCI DSS = payment Gateway Security policy.

(NIST)

(Sniff)

Access Control :

Authentication ⟶ credential ✓

Authorization ⟶ what you do after authentication

Ways to implement Access control :

Attributes based access control.

MAC - Mandatory Access Control ⇒ Not flexible
→ ~~its~~

↓

To change
access control
change the policy itself.

TAC

RBAC - Role Based Access Control

↳ Roles will have access control,
not the individuals

ABAC (Attribute Based Access Control)

25th Oct 2023

Access Control policy is a subset of whole policy

30th Oct 2023

Computer System Security

- Planning. => when we deploy OS
  1. Risk Analysis
  2. Security Policy & procedure.
  3. Security Awareness Training
  4. Incident Response
  5. Compliance & Regulation.
  6. Budgeting.
- Hardening
  - Operating System & Hardening.
  - N/w Hardening
  - Application hardening
  - Access Control
  - Data Encryption
  - Patch Management
  - Vulnerability Mngnt
  - Security Testing.

Maintenance

1. Regular Updation & Patching
2. Log & Event Monitoring
3. Incident response
4. Back Up & Recovery
5. Documentation.

Dec 20

Attack Surface

↓

which allows someone to enter.

Web Application

* 1st Oct 2023

(M1) (M2)

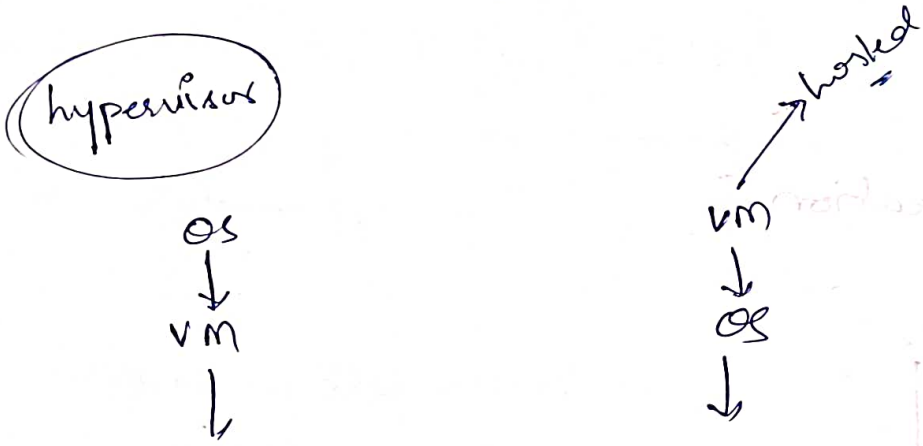
ring principle of privilage seperation will be more secure.

Broken Access Control Vulnerability

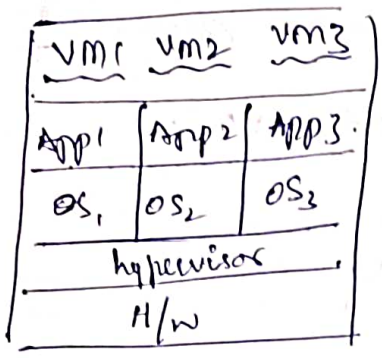
3rd Nov, 2023

Virtualization

2 kind → Hosted Virtualization
       → Native "

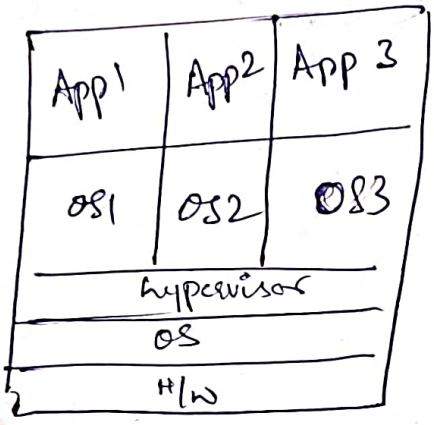


6th NOV, 2023



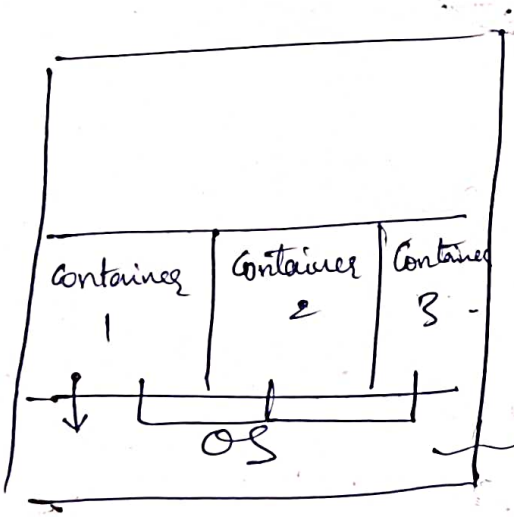
hypervisor directly installed on H/W

Base Model Virtualization.



hypervisor installed over OS.

Hosted Virtualization



Most vulnerable cause of one container gets accers of os then it can have access of other containers.

Docker /

Linesofcode are less

In terms of isolation, Docker is more vulnerable.

In terms of line of code, Hosted

isolation > line of code.

Docker is more vulnerable than Hosted.

→ In hosted & Bare Metal, one OS can communicate with other iff one VM has shared resources with other.

→ We measure the ~~hypervisor~~ isolation is done with hypervisor. with accessing hypervisor.

→ How do reduce the surface of attack?

① Hardening: without using default settings while installing.

② Maintaining:

→

① Vulnerability in host OS
② Inter VM connection
③ VM-Escape Vulnerabilities
④ M.S configurations
⑤ Outdated s/w
⑥ physical Access
⑦ Privilege Escalation.

Extreme Users Authentication

As the no. of factors ↑ ⇒ security ↑ ⇒ usability ↓

factor: no. of ~~characters to access in a password~~ levels to access smtg.

Like "2-factor verification of GOOGLE".

→ password vs Biometric ?

password > Biometric ; Biometric once leaked can't be changed

---

8th Nov, 2023

Electronic User Authentication

↳ Password Based Authentication

↳ Token " "

↳ Biometric " "

Risk Assurance:

↳ one factor → load 1 assured

↳ ~~one~~ 2 factor → load 2 "

↳ 3 factors → load 3 "

① Dictionary Attack: ⟶ Dictionary of common passwords
(available on internet

② ~~Rainbow~~ Ringo → Not calculating hash same time at Runtime
Rainbow table Attack

Here the maintain the hash of common passwords

This removes the solution for Dictionary Attack

To overcome this problem people started to store the hash of passwords instead of normal storage in tables.

Then what should we do?

Now, we can add a "KEY" to the hash, which will be unique for each user.

Adding KEY to the password is called "Salting"
(after this then the whole stuff is hashed.

Adding unique key results in increase in search space.

What to do if the attackers gets to know what key is used for each password?
↳ what to do so the key is not disclosed?

Pepper ⇒ we will add another key to not disclose the salt key. and the pepper key is same for all.

Token Based Authentication:

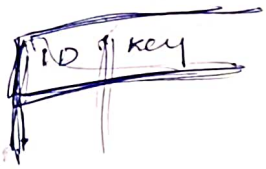
Ex: Debit Card

2-factor (Security: Authentication)
- 1. Card → Gives ID.
- 2. Password.

Digital Signature is not the best solution to ~~do~~ use for mobiles. Cause ~~the~~ it is complex & stuff..

↓

We use MAC with symmetric key for authentication



↓

What are attacks that are possible here?

↓

Hold on key can cause a problem.

To overcome this we can do encryption to the table, with a key

↓

Can we do Hashing here?

No, hashing doesn't provide confidentiality it only maintains integrity

Biometric

10th NOV. 2023

fingerprint ⟶ registered at server.

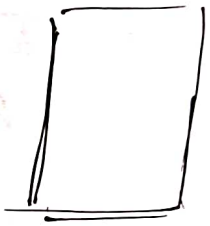
2 Types → Static : Thumb / Irris
→ Dynamic : Voice

We can convert 2-factor to 3 factor by adding ~~fingerprint~~ biometric into the process

This is more secure & less usable.

Applications

- Mobile



Base Stations

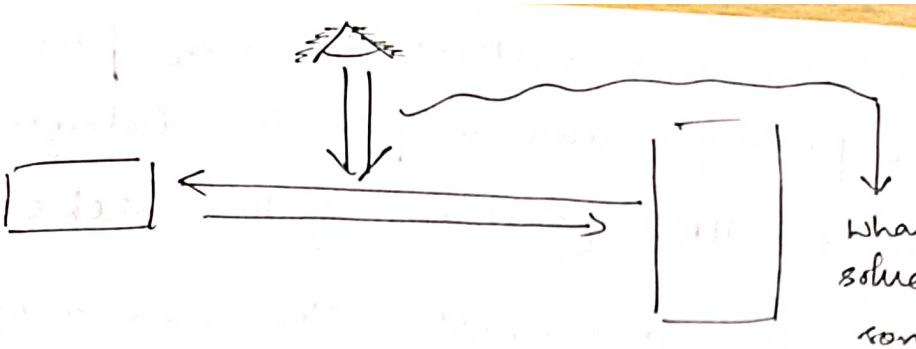
what should be done for authentication?

There is a key present in the phone handshake There is no need to exchange the key.

"key exchange is out".

Symmetric ✓ / Public-private ✗ ⇒ Symmetric key

MAC ✓ / Digital Sign ✗ ⇒ MAC ∵ Computational power.
∴ we need 3rd party in Digital Sign.



What do we do to solve this problem of someone watching / hearing info?

We use public-private key to solve this

15th Nov, 2023

Q: A company named X wants to offer a server cloud, based backup system. When the user updates a local file, her client opens a TCP connection to the X-servers and uses the Diffie Hellemen protocol to establish a secret symmetric key K with the server. Then the client guarantees the string s_i

(1) $S = \{$documentName, Username, userPassword, randomNumber$\}$

and sends the following ~~msg~~ message to the X servers.

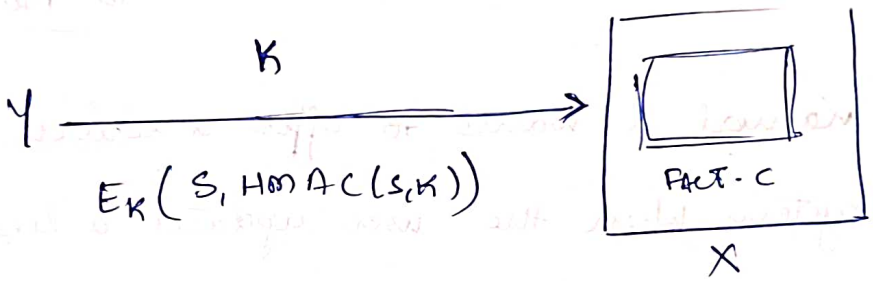
$$E_K(S, HMAC_K(S))$$

where $E_K(m)$ denotes ~~everything~~ encrypting messages in using key K, & $HMAC_K(m)$ denotes computing an HMAC message authentication code of msg in using key K. (2)

The server decrypts the msg, verifies the user password and verifies the user password and verifies the integrity of the msg. using the HMAC (3)&| all of the checks succeed the server stores the document. How can a n/w attacker obtain the user password.

Ans:

Diffie Hellmen exchange



Cloud Based Backup System

Random No | Time stamp are used to avoid Replay attack.