Digital Signatures : Diffie hellman

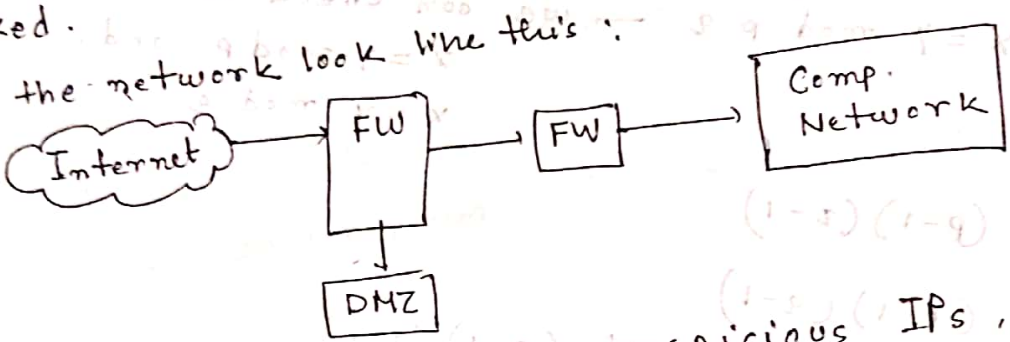
—·—

Sohrab Sir (class 2) :

(x) DDoS Attack (Can't change data, but makes server broken)

Aug 15, 2023 : ORG (birth registration) information of Bangladesh got leaked.

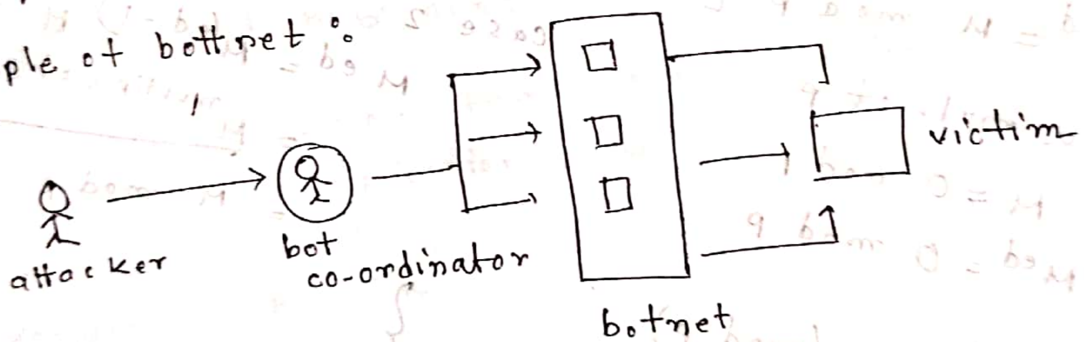
Generally the network look like this :



Cyber threat intelligence : Tracks suspicious IPs, by doing data mining,

(ii) How can you find out that whether my device is bot or not?

Example of bottnet :



(i) Performance drop

(ii) CPU usage (when only broswer but high usage)

(iii) Wireshark (track connection)

Prevention : HIDS (Host intution detection System)

Honey pot : অনেক computer থাকে critical infrastructure company হয়

Phishing link
Social engineering attack

Sohrab-Sir (Class 1) :

Basic concept : Whether we can attack (VS) how can we defend
(Red vs Blue)

Some of the computer security researches are done by military fund.

Top 10 cyber attack :

Before internet, computers were completely isolated. After that the era of unauthorized access began.

2007 Estonia : Due to cyber attack, we had unprecedented amount of traffic. By random users. This is known as Denial of Service (DoS), by using thread programming. এক computer থেকে website এ different port দিয়ে access করা।

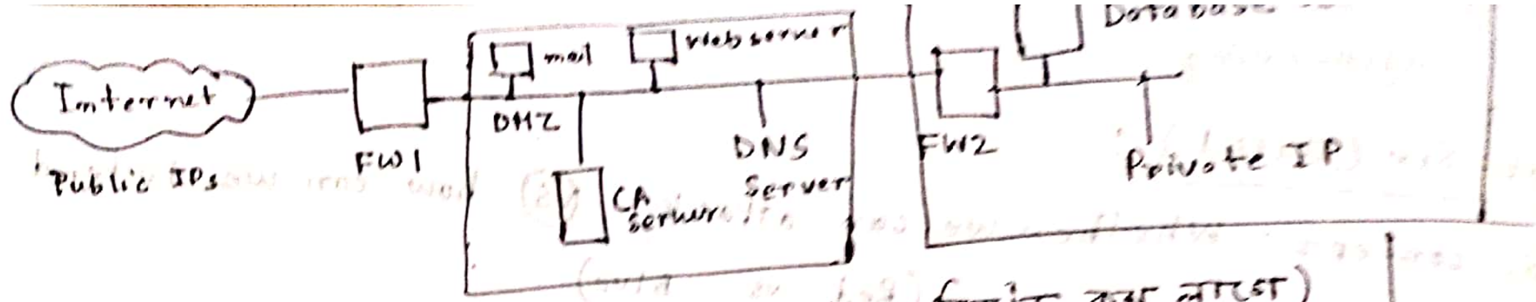
How to identity a TCP session ?
(SrcIP, SrcPort, DestIP, Destport)
↳ 16 bit port, so we launch DoS attack against BIIS but creating port 1000, 1001 . . . . 65535)

To prevent DoS attack, BIIS can block traffic itself (for example by limiting to session time / no. of users). But bank can't do that, otherwise customer will go to other bank.

So, we have to detect illegal traffic from the legit users.
Also, we can prevent DoS attack from a certain IP by using firewall. By block sourceIP = X.

As a way around, attackers do DDOS (distributed . . .)
How ? ① by hiding the IP
② by using botnet

(attacker does not attack directly, এভাবে attack করলে সে website block করে দিবে)



De-mitilarized zone (যেখানে security নিয়ে কম ভাবতে)

MP
(with most sensitive information)

Mail /Web server are in DMZ, because they are directly accessible from the outside.

Botnet: The attacker uses malware in different people's devices. Then attacker can control those devices to do attacks on victim (website). Bottnet can be done worldwide!

Now, website can't stop literally all of the IPs. So, firewall can't prevent this.

2. 2015 – Ukraine Power outage: Power plants were attacked.

3. Nasa Computer by creating a backdoor. For example, I created an account with admin access, then I can just enter the website legally.

MSH (class 3):

Security goals → Availability, Confidentiality, integrity.

Trade off for security is usabilility

Virus goes beyond OS and reaches privilege mode so, we can't just delete it. Example: rootkit

Crypto-analysis → try to decrypt without using key.

Tools for confidentiality: Access Control

Authentication: You know - You have - You are

Authorization:

grant 'select on customer' to Alice

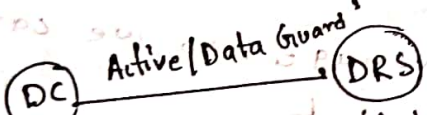
↳ Now, alice can read the customer table but can't write

like Farady cages → Electromagnetic signals can not enter or exit the enclosure

DC → data center

For example DRS (Disaster Recovery site)

Data should always be kept in a different location. otherwise in a disaster, both main and backup will be corruption.



↳ Quick backup and sync

Active - - - - - Active (Hot stand by)

DRS will start working when DC is down

Active - - - - passive (cold - stand by)

↳ taken some time to be on

Active - - - - - Active (warm stand by)

(written at the end of the day)

if availability is increased → cost ↑

AAA

↳ Assurance, Authenticity, Anonymity,

Class - 4 :

Assurance: Service provider বা service provide করছে, it is trustable? There can be some privacy related issues. For example, we are giving ID, password, NID as input. These should be kept with privacy.

Authenticity: To check genuine or not. For example a letter issued by client, must be verified. For example, email from NBR to pay in an account.

Sol.: We have to use digital signature. Alice ⟶ Bob, the bob must make sure it was from Alice and alice can't deny it later on.

Anonymity: We want some things to be annonymus. For example, providing a servery, so we can't identify exactly who submitted that.

Tools: 1. Aggregation : Sum | average

2. Mixing 3. Proxy 4. Pseudoanonymous

(for example we need avg; but don't want to reveal the identity and his CGPA)

reality:

A 3.8
B 3.9
Avg : 3.85

Mixing ⟶

A 3.9 or 3.7
B 3.8 or 4.0
Avg : 3.85 avg : 3.85

desired data same

Alice ——— Bob

eve

Eavesdropping.
If weak encryption, eve can find out the sent data.

ping www.google.com

tracert www.google.com → shows all the routers in the path.

That's why many countries don't communicate their channels over hostile countries. (fear that govt can eavesdrop)

Alternate:
① Alt. route ② Satellite link (Satellite constellation: A set of satellites)

Example: GPS

Recon: By using satellite images, we can identify the movement of heavy vehicles (heavy armor movement indicates war)

MITM (Man in the middle) attack: Unauthorized modification of information.

Masquerading: - From Alice (but actually it was from eve)

Repudiation: denial of a commit or data receipt.

We want non-repudiation.

Spoofing: কেউ আমার নামে কাউকে message পাঠাচ্ছে।

- IP-spoofing
- MAC-spoofing
- DNS spoofing
- DHCP spoofing (DHCP server assigns IP and nearest gateway router. by spoofing, attacker can change the default gateway to the router of hacker)

To track spoofing, we use co-relation and trackeback.

10 Main Security Policy:

① Economy of mechanism: By using simple security policy, it's more user friendly

⑪ Fail-safe default: Default new user should have minimal privilege, not have 50%: admin power. আগের SW তে এমন ছিল because everyone is trustable. Forex: In ARP, we want MAC of B, instead আগের believe না করে of B. C sents his own MAC.

(III) Complete Mediation : Every action must [illegible] for security. We have to check whether the request is valid, so we have to add all these policies (corner case)

(IV) Open design : Our secu Arch and design should be publicly available, only the key is secret. If we keep open design, our system can be scrutinized by other parties.

└ Opposite : Security by obscurity (this is also a form of security, for example propiertary designs, military techniques)

Class → Graphics editor

⊗ ~~If~~ audit : Audits the codebase for security check.

Approximate ~~possible~~ character password ~~is~~ maximum possible combination (length = 10) → $(32 + 32 + 10 + 32)^{10}$

upper, lower, number, special char.

So, if password expires in every 30 days,

hacker has to make : $\frac{94^{10}}{30 \times 24 \times 60 \times 60} \approx 3$ trillion / second

↓

Server even can't authenticate that fast.

Dictionary attack is a type of password attack.

Also, attack type depends on protocol (SMTP, FTP). For example, each type of application have different headers in each protocol.

Social Engineering → Pretexting
→ Baiting
→ Quid Pro Quo

Computer Forensics : Crime হলে তার investigation.

↳ used as digital evidence (by IO investigating officer)
↳ Process of preserving, identifying, extracting, documenting and interpreting data on a computer.
↳ each hard drive has a hash, so IO can't change the evidence itself.

LI : Lawful interception of phone calls.

Identification of evidence : If pc is on we can take the snapshot of ram. In general, hard disk, SSD is a must. Mobile phone, pen drive. (does not require much time)

Collection : We can't just copy evidence to our device (it will change the modification date when we work on that copy, so, we keep a master copy and work on other files). The act of copying in known as imaging (bit by bit copy)

Write blocker : Source থেকে copy করার সময় যাতে device. It will not change any data of the source. It uses source as read only.

We still need traditional forensics analysis. (for example, we can still get actual fingerprints), on fingerprint on laptop screen.

Analysis and Evaluation : Forensics tools : Autopsy, Encase

To maintain integrity of evidence, we keep hash of the evidence. If investigation officer changed the evidence, the hash will also be changed.

Chain of custody form → search google

Priority by volatility : RAM > swap > disk > CD/DVD
↑ more important to capture first.

if we found a computer on, connect battery immediately as that the comp stays on (if comp. gets off, we can not get the RAM image)

Analysis and evaluation :

If I want to protect info, ways are
(attack)
- changing .txt to .JPG
- hidden files
- Encryption
- password

in attacker's PC, we have to check the recycle bin, internet history, downloads, temporary internet files, saved passwords ;.

Hackers can use "zeroize" for anti-forensics. it will replace the data with all 0. so, in forensics, in autopsy, it can't find the file.

Spool files → যেকোন file print করার জন্য printer এ spooler directory তে জমা হয়ে থাকে।

How to hide data?
- Cryptography
- change file extensions
- steganography
- deleted files
- hidden tracks.

Reporting : Must be done in, with details. It should provide evidence to stand against scrutiny.

* What if :

User	Password
A	abc123
B	abc123

→ hash will
Attacker will get a

So, we hash → ~~Attak~~ A + abc123 } so, it looks
B + abc123 } different when hashed.

Sohrab Sir :

Forensics tools : enCase, Autopsy, Velociraptor

Ghost image : In file system, files are linked with each other. Unless we overwrite them with 0, it's possible to find data from deleted files.

File System Security :

Discretionary Access Control (DAC)

- The owner may grant access to other, control access

Close System → by default all deny, then we can specify access.

Reporting must be done professionally with proper format. Otherwise it would withstand legal scrutiny. Must also have a conclusion and logics around it.

The criminal will do anti-forensics technique. In case of descructive erase, all data in the file is overwritten.

Open Policy → By default all allowed. We have to specifically deny them.

By linux, default → closed system.

In ACL, we have to do specific first and then generic

deny host 192.168.10.10

allow 192.168.10.0/24

linux: d/d1/a.txt

if we have access here and not for d1, we actually can't execute it.

windows: a.txt ☞ permission ... enough.

linux considers every thing as file.

Hard link

(if all hard links deleted main file gets deleted)

Soft link

↳ delete ... no problem in original file

(like windows shortcut)

File sharing Challenge:

chown (change ownership of file)

chown tom:GroupX a.txt

↳ owner and group both changed.

Hackers normally low privilege ... access ... And then does privilege escalation to reach root. Then perform chown, chmod ...

sudo → used to get the privilege of the root user

special permission:

set-user-id (

rwx / rwx / rwx

owner/user / group / others

rws

(we can convert execute to set-user | set-group ID)

For example, in usr/bin/passwd we have rws so it has the privilege of root Although Bob is using it. but in privilege of root.

if we login as root, ... login as bob.

passwd tom sudo passwd tom.

enter pass: ROOT-PASS enter pass: ROOT-PASS

Usually we don't directly login with root. Since a wrong command in root can be harmful.

Now,
→ Bob@BUET $ passwd
> old pass :
> new pass :

in normally pass
etc/passwd.
etc/shadow has the hash value of the password.

{ /usr/bin/passwd → Exec
/etc/passwd → txt file

in shadowfile :

sojib $ id $ salt $ hashed $ last pass change
↓ means which type of hashing

↳ if no salt :
bobpass : CSEBUET
alicepass : CSEBUET
so, for both :
$1 $ Hashed
$1 $ hashed.

so, we have to use salt
using 'S' is not useful

Adding a 'T' (sticky bit) means this file can be read/executed by everyone but not renamed or deleted

—o—

One man army → Single person doing all the coding, testing debugging, reviewer. This is of course not recommended.

80-20 rule | 90-10 rule

first 80% work time = last 20% work time (includes testing...)

fix ↔ bug

Authentication :
person → has : OTP
→ is : Fingerprint, eye
→ knows : password