Network Security

Types of Encryption

Symmetric - for large data
Asymmetric - for personalized data

CIA - forms the basis of Security

Confidentiality | Integrity | Availability

CIA is also called the Security Triad.

IETF - Internet Society

OSI - standard that defines the different layers of a computer network.

RFC (Request for comment) ⇒ Recommended
Required
Elective
Useful.
Not Recommended

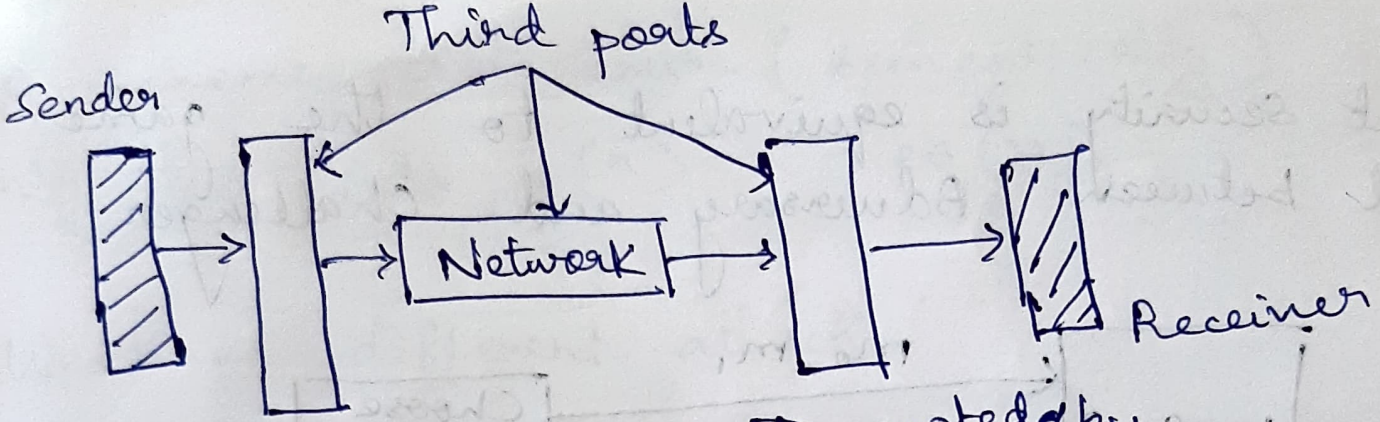
Types of attacks

Passive attack.

- Releasing sensitive information
- Traffic Analysis

Active attack

- Masquarade
- Replay
- Modification of Message
- Denial of Service


Third parties
Sender
Network
Receiver
Encrypted / Transformed by Security Mechanism
Decrypted by Mechanism

Network Security

Security issues in TCP/IP suits:

(i) Sniffing / Eavesdropping (in routers)

(ii) Spoofing

(iii) Buffer overflow

(iv) Illegal packets → Ping of Death

(v) ARP poisoning → Man in the middle

(vi) Denial of Service / Distributed DOS

(vii) ICMP Exploits → Echo
→ DOS
→ Flooding
→ Ping of Death

Security issues in IPv4:

IPv4 doesn't check whether source address is correct or not. It assumes that data is coming received from the correct source without verifying it.

The exploitation of this limitation is called spoofing.

IPv4

→ Spoofing

→ IP fragment attack

In spoofing, router has to check if the packet's source is correct and if it actually exists.

IP fragment attack

IP fragments are overlapped with other IP fragments. This results in DoS. This is often used in bypassing firewall.

Routing Exploits

→ Packet mistreating attack

→ useless packets are sent to the router

→ modifying routing table

→ Hit and run: Hit the router, if access is yes, continue else go away.

→ Persistant attack: Keeps on attacking Router until it breaks the firewall of router

UDP Exploits

→ Flooding

(2 services chargen (port no. 19) and Echo (port no. 7) are used

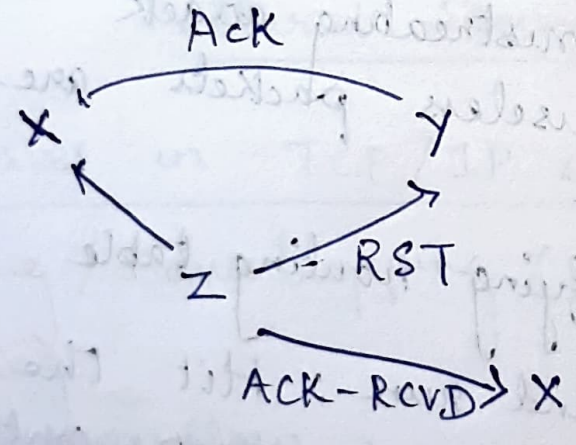
Broadcast address is used to as source address to generate large data, which is sent to the port no. 7 of the server. The server returns the data back)

TCP Exploits (~~Shred Attack~~)

- Sequence number prediction.
  (~~Algorithm~~ Random algorithm that generates the initial sequence number is predicted by attacker)

- Closing connection
  (Attacker changes TCP flag to FIN. The receiver closes the connection as it found the FINS flag. This results in loss of packets)

- TCP ~~Attack~~ RESET attack



Network Security

Acknowledgment Trick

congestion window gets reduced if 3 duplicate acknowledgment packets are ~~red~~ received.

- ACK division
- Duplicate Ack spoofing
- Optimistic Acknowledgment

Illegal Segments

SYN and FIN flags are sent together

Attacker $\xrightarrow[SYN+FIN]{}$ V

SYN

↓

SYN-RCVD

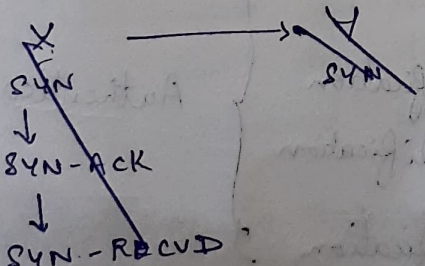
↓

FIN → CLOSE WAIT

Sender will be in a half closed state waiting for ~~receiver~~ acknowledgment from receiver.

Simultaneous connection

Both sender and receiver send SYN Segment to each other



X $\longrightarrow$ Y (Here Y has to send SYN-ACK)

SYN

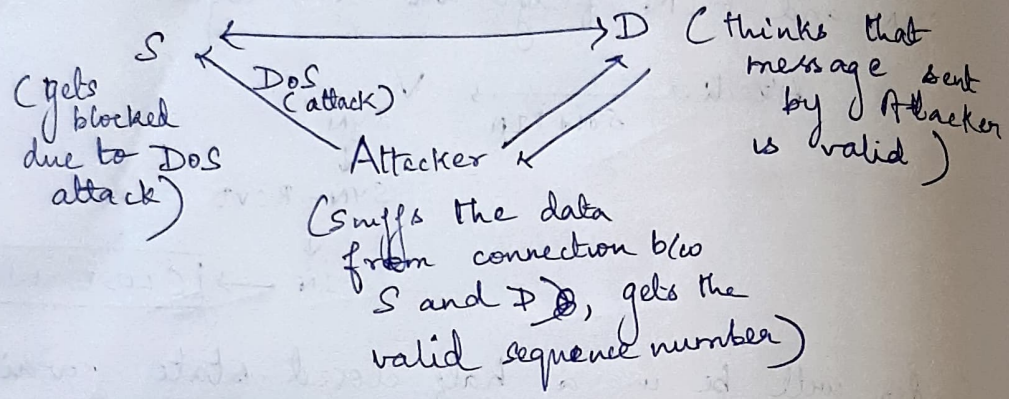
But if Y has a malicious intent and sends SYN only, X treats it as Simultaneous connection request and goes directly to SYN-RCVD state. This state doesn't have

any times. So, X gets stalled indefinitely leading to denial of service.

Connection flooding / SYN flooding

- Simultaneous connections are opened with all ports in a server.
- this attack becomes more dangerous with IP spoofing.

Connection Hijacking



Message Authentication

1. Disclosure
2. Traffic Analysis

} confidentiality

3. Masquarade
4. Content modification
5. Sequence modification
6. Timing modification

} Authentication

~~7. Source modification~~

7. Source Repudiation
8. Destination Repudiation

Social Engineering

- Bailware
- Scareware
- Phishing
- Spear phishing
- Pretexting

Phishing - obtaining user information by creating a ~~fake~~ duplicate website

~~Spear phishing~~ -

Social Engineering involves manipulating the psychology of the victim to steal their information.

Message Confidentiality

- Disclosure
- Traffic analysis

Masquarade - pretending to be the sender

Digital Signature

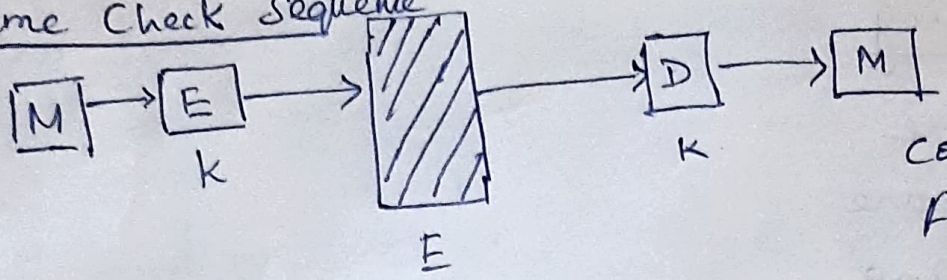
- Source repudiation
- Destination repudiation (~~user~~ receiver can't deny that they have received the message)

Different methods to ensure ~~a~~ destination function

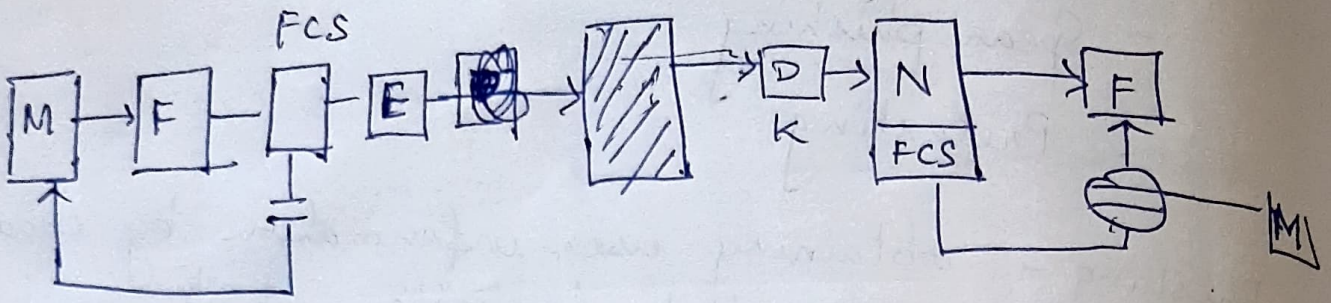
1. Hash ~~function~~ function
2. Encryption
3. ~~MAC~~ MAC (Message Authentication code)

Hash function - maps any message of arbitary length to a fixed length number.

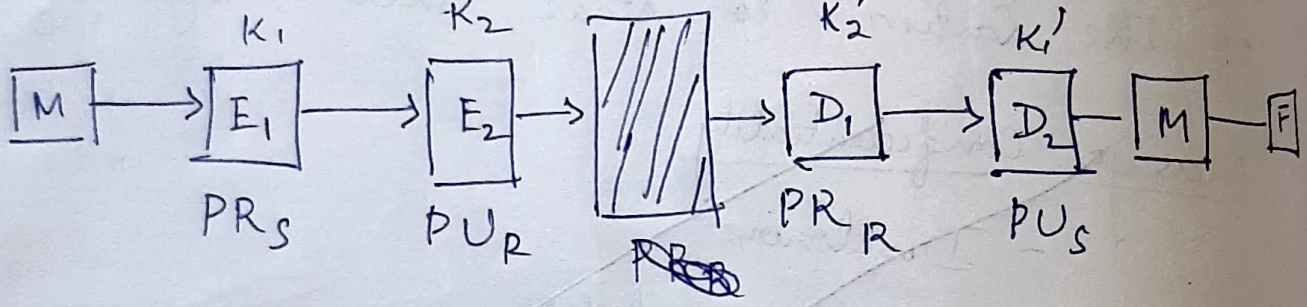
Frame Check Sequence



provides both confidentiality, and Authentication



Using 2 keys to ensure ~~both~~ authentication ~~and~~, confidentiality and Signature



However, the above asymmetric encryption is costlier.

Message Authentication Code

$$MAC = F(K, M)$$

MAC: tag (similar to checksum)

F: Many-to-one

Network Security

MAC (Message Authentication code)

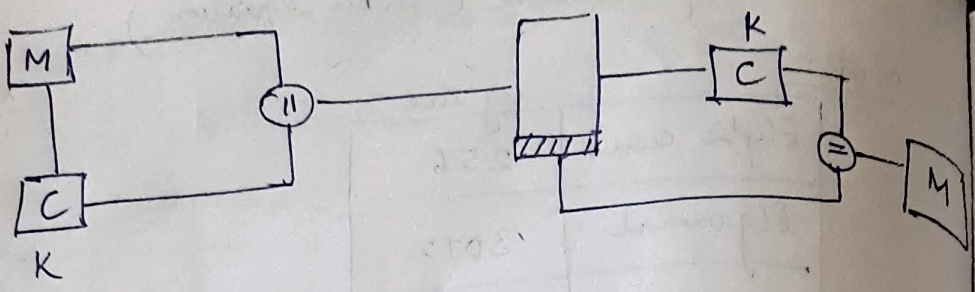
- A many-to-one mapping
- fixed length code

$$MAC = C(K, M)$$ [Symmetric key encryption]

K – Encryption key

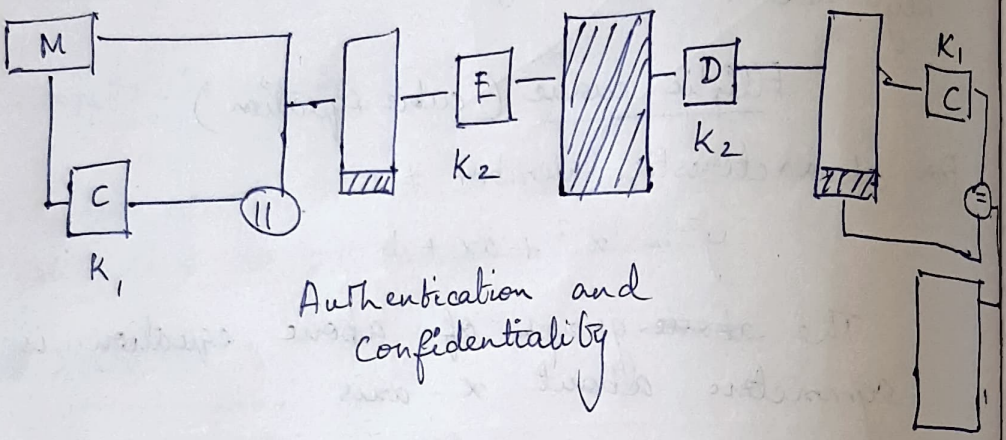
M – Message

- It is a cryptographic checksum / tag



- This will provide only authentication and not confidentiality because message is not encrypted

- To provide confidentiality:



Authentication and Confidentiality

MAC is used instead of encryption because

(i) cost effective
(ii) fixed length output
(iii) It is a many-to-one ~~mapping~~ function.
(iv) random sample can be checked for correctness of MAC.

Since MAC = C(K, M) is a many-to one function, many keys may give the same MAC value.

Uniform distribution of MAC function

The mac functions should be equally distributed. There should be no bias between functions.

$$Pr(MAC(K_{01}, M_1) = MAC(K_{02}, M_2)) = 1/2^n$$

$$Pr(MAC(K, M_1) = MAC(K, M_2))$$ [It must be computationally difficult to find K in this case]

$\min(K, n) = 128$, so that bruteforce takes atleast 2^{128} attempts.

Cryptanalysis : $1/2^n$

Computational resistence $\Rightarrow$ ~~MAC~~ $MAC(x_1, K_1)$
$MAC(x_2, K_2)$

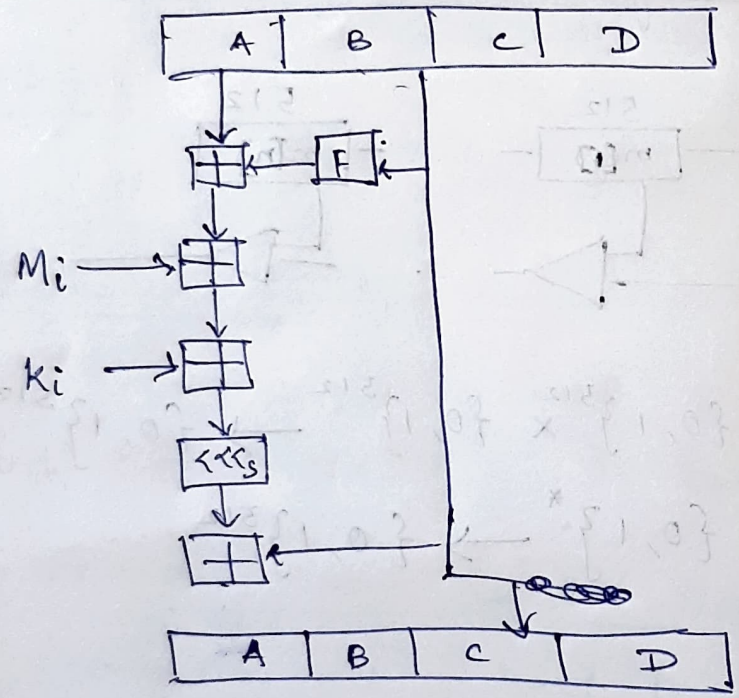
$$K = \min(2^K, 2^n)$$

A function $f(x)$ is linear if

$$f(x+y) = f(x) + f(y)$$
$$Kf(x) = f(kx)$$

Note:

AND, OR, NOT are non-linear functions
XOR is a linear function



Problem

~~Padding = 512~~

$$(|M| + |P| + 128) = 0 \bmod 1024$$

$$\Rightarrow |P| = (-|M| - 128) \bmod 1024$$

$$|P| = 354 \text{ bits}$$

2590
128
-2718
3072
2718
354

Network Security

For SHA-512, the entire input is divided into 16 words of size 64 bits each.