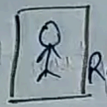
2) ACTIVE attacks

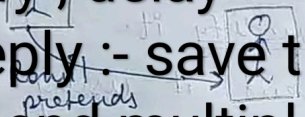
It attempts to alter system resources / info

(i) masquerade

→ when one entity pretends

eg





(ii) modification of messages

some portion of message is delayed or reordered to produce unauthorized effect

(iv) Denial

It p

eg

Active attacks

1:- Masquerade:- someone other

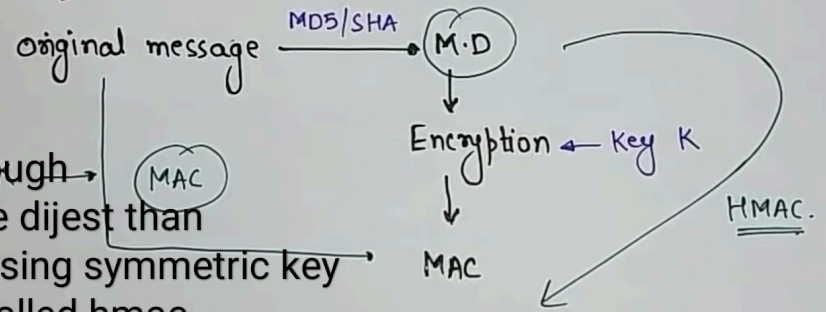
2:- Modification of message:- modify , delay

3:- Reply :- save the message and send multiple times

4:- Deniel of service:- To much requests on server

HMAC [Hash-Based Message Authentication Code]
used for Security implementation in Internet Protocol(IP) and also in SSL(Protocol). → Secure-Socket Layer.

Concept of HMAC:



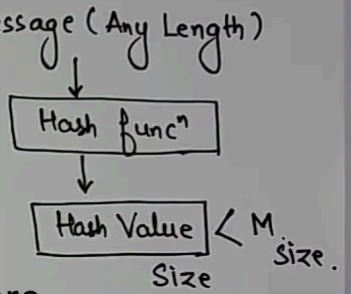
If we go through 1st message dijest than encryption using symmetric key using algo called hmac

HASH FUNCTIONS: [Compression func^n]

It is a mathematical func^n that Converts a numerical i/p value into another Compressed numerical value.

(i/p) 10
(o/p) (4 bit) 12
:
50

↳ o/p is always of fixed Length.



Features:

Message Value generated are called message digest no matter how much length of input if hash function of 4 byte then answer is of 4 byte

Properties: (i)

(ii)

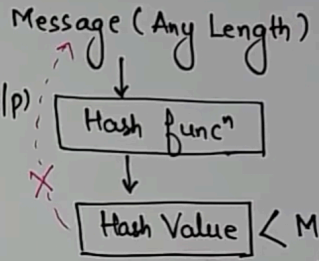
(iii)

HASH FUNCTIONS: [Compression func^n]

It is a mathematical func^n - that Converts a numerical i/p value into another Compressed numerical value.

(o/p) (4 bit) ← 10, 12, ⋮, 50 (i/p)

↳ o/p is always of fixed Length.



Features:

(i) fixed Length o/p
(ii) Compression func^n
(iii) Digest (Smaller rep^n of larger data)

Reverse hash must be impossible
2 ka hash same na ho
same value ka hash same aya

Properties: (i) M ⟶ H (Easy) H ⟶ M (Very Hard)

(ii) M ⟶ H, ⋮, n ----> H } Same hash value for same message everytime.

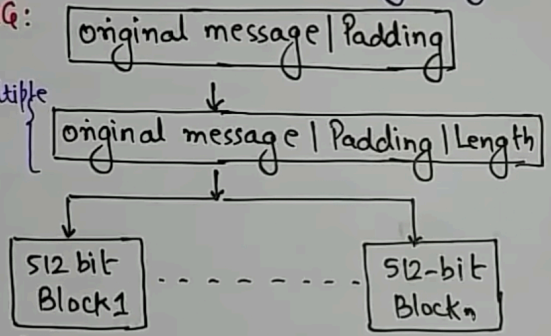
(iii) $M_1 \longrightarrow H_1$, $M_2 \longrightarrow H_2$] $H_1 = H_2$ should not happen.

MD5 [MESSAGE DIGEST]

↳ developed by Ron Rivest.

↳ Fast and produces 128-bit message digests.

WORKING:



(i) Padding is done such that total length is 64 bit less than exact multiple of 512.

1000 bits + 472 = 1472

512 × 2 = 1024

512 × 3 = 1536

64

1472

64 bit less than exact multiple of 512.

(ii) Append original length bef. padding (modulo 64)

1000] length mod 2^{64}.

(iii) Divide it in 512-bit blocks.

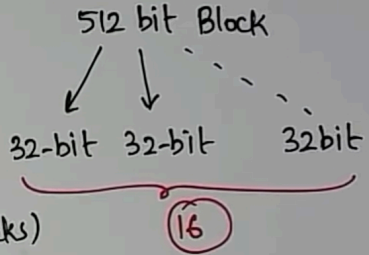
(iv) Initialize 4-Chaining Variables. (32-bit, A, B, C and D)

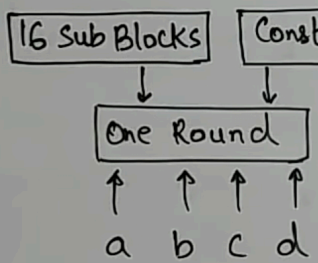
(v) Process Blocks

↳ Copy four chaining Variables into Corresponding Variables.
{A=a, B=b, C=c, D=d}

↳ divide 512-bit block into 16 (32bit blocks)

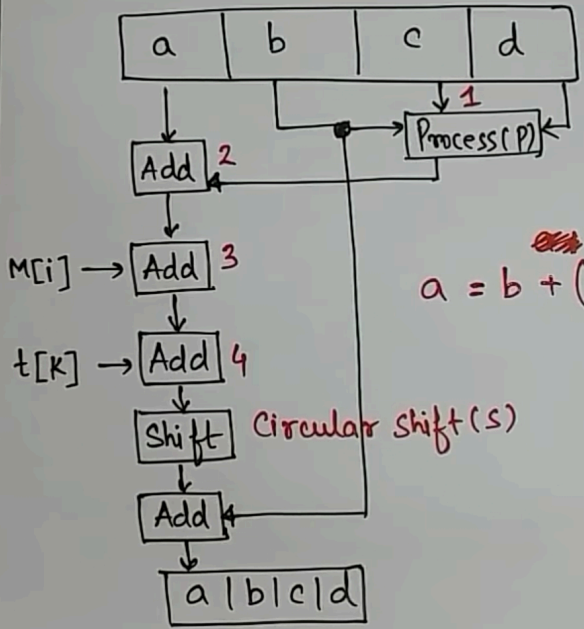
↳ Four Rounds.





$a = b + ((a + \text{Process}_P(b,c,d) + M[i] + T[k]))$ ≪ shift.

MD5 Operation:-



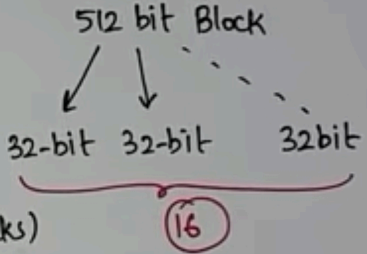
$$a = b + (\text{Process}(b,c,d) + M[i] + t[K] \ll s)$$

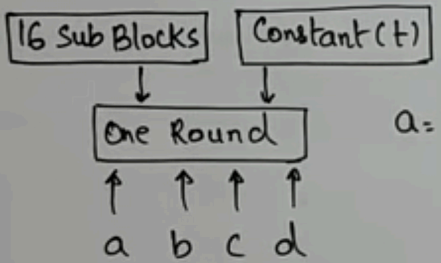
(v) Process Blocks

↳ Copy four chaining Variables into Corresponding Variables.
{A=a, B=b, C=c, D=d}

↳ divide 512-bit block into 16 (32bit blocks)

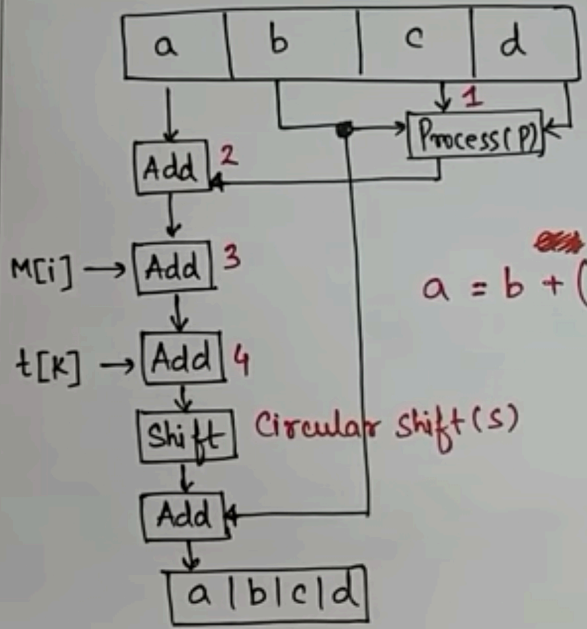
↳ Four Rounds.





$a = b + ((a + \text{Process}_P(b,c,d) + M[i] + T[k]))$ ≪ shift.

MD5 Operation:-



$$a = b + (\text{Process}(b,c,d) + M[i] + t[K] \ll s)$$

→ HMAC ALGORITHM

Authentication:

Hashing → X keys

mac → keys

Hash + mac

Hashing with keys

1. compote S-bits → Key (K)
2. S || M
3. Hash function

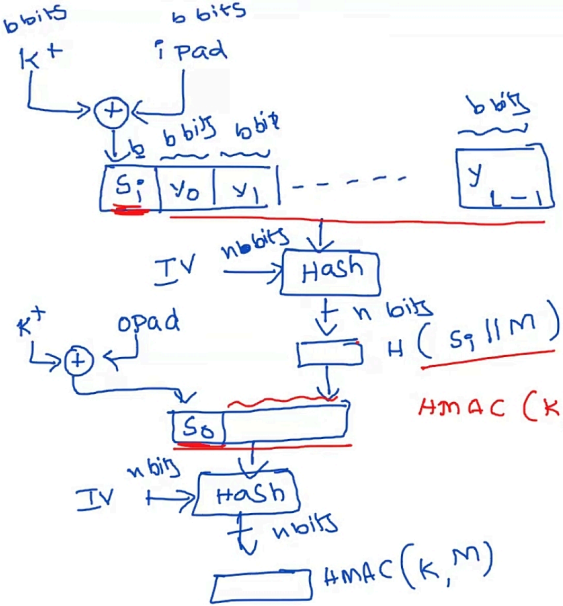
Block size of plaintext → b bits

K → K^+ (b bits)

100

70 → 30

- ipad — 36 hexadecimal — 0011 0110
- opad — 5C hexadecimal — 0101 1100



IP

M - PT

V_i = i th block of M

L - no of blocks in M

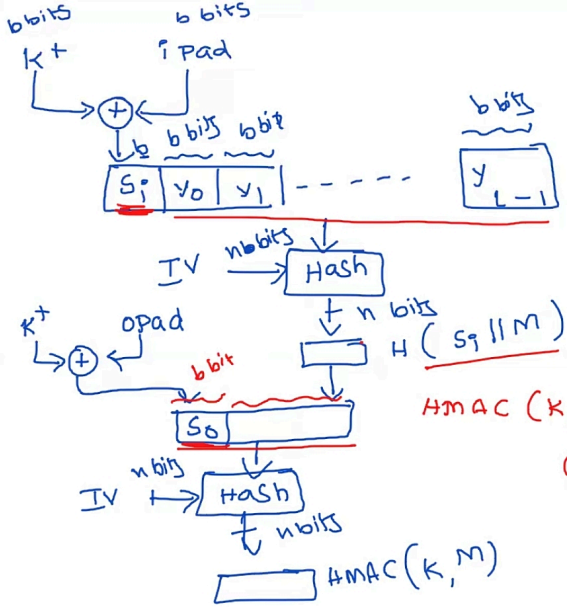
n - length of the hash code

H - Hash function

b - no of bits in a block

K - key

$$HMAC(K,M) = H\left[(K^+ \oplus opad) \,||\, H\left[(K^+ \oplus ipad) \,||\, M\right]\right]$$



IP

SSL

M - PT

Y_i = i th block of M

L - no of blocks in M

n - length of the hash code

H - Hash function

b - no of bits in a block

K - key

$$HMAC(K,M) = H\left[(K^+ \oplus opad) \| H\left[(K^+ \oplus ipad) \| M\right]\right]$$

1) Append 0's to left end of K → K^+
2) XOR K^+ with ipad → S_i
3) $S_i \| M$
4) Apply H — step 3
5) XOR K^+ with opad → S_0
6) $S_0 \| \ldots$

ElGamal Cryptography: Asymmetric Key.

i) Key Generation:

i) Select Large Prime no. (P) ⇒ P = 11

ii) Select decryption Key / Private Key (D) = 3

iii) Select Second part of encryption key or public Key (E1) = 2

iv) Third part of the encryption Key or public Key (E2). $E2 = E1^{D} \bmod P$. ⇒ 8

v) Public Key = (E1, E2, P), Private key = D

⇒ (2, 8, 11), ↳ 3

ii) Encryption:

i) Select Random Integer (R) ⇒ 4

ii) $C1 = E1^{R} \bmod P$, $C1 = 2^{4} \bmod 11 = 5$

iii) $C2 = (PT \times E2^{R}) \bmod P = (7 \times 8^{4}) \bmod 11$

iv) C.T = (C1, C2) ⇒ 28672 m

iii) Decryption:

$PT = [C2 \times (C1^{D})^{-1}] \bmod P$

P = 11, D = 3, E1 = 2 | P.T = 7

$E2 = (2)^{3} \bmod 11 = 8 \bmod 11 =$

C1 = 5

ElGamal Cryptography: Asymmetric Key.

i) Key Generation:

i) Select Large Prime no. (P) ⇒ P = 11

ii) Select decryption Key / Private Key (D) = 3

iii) Select Second part of encryption key or public key (E1) = 2

iv) Third part of the encryption Key or public key (E2). $E2 = E1^{D} \bmod P$. ⇒ 8

v) Public Key = (E1, E2, P), Private key = D

⇒ (2, 8, 11), 3

$(125)^{-1} \bmod 11$

$(125 \times x) \bmod 11 = 1$

$x = 3$,

ii) Encryption:

i) Select Random Integer (R) ⇒ 4

ii) $C1 = E1^{R} \bmod P$, $C1 = 2^{4} \bmod 11 = 5$

iii) $C2 = (PT \times E2^{R}) \bmod P = (7 \times 8^{4}) \bmod 11$

iv) C.T = (C1, C2)

⇒ 28672 mod 11

⇒ 6

iii) Decryption:

$PT = [C2 \times (C1^{D})^{-1}] \bmod P$

P = 11, D = 3, E1 = 2 → P.T = 7

$E2 = (2)^{3} \bmod 11 = 8 \bmod 11 = 8$

C1 = 5, C2 = 6

7 → Encryption → C.T = (5, 6) → Decryption

$PT = (6 \times (5^{3})^{-1}) \bmod 11$

$\Rightarrow (5^{3})^{-1} \bmod 11 \Rightarrow 3$

$(6 \times 3) \bmod 11 \Rightarrow 18 \bmod 11$

PGP-1

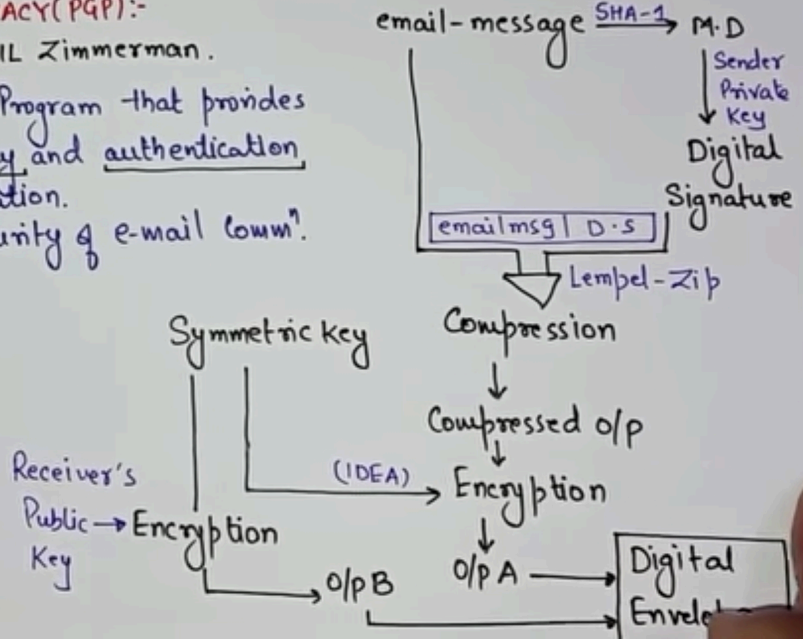
PRETTY GOOD PRIVACY (PGP):-

Father of PGP = PHIL Zimmerman.

It is an encryption Program that provides cryptographic privacy and authentication for data communication.

→ Increases Security of e-mail comm".

PGP WORKING:



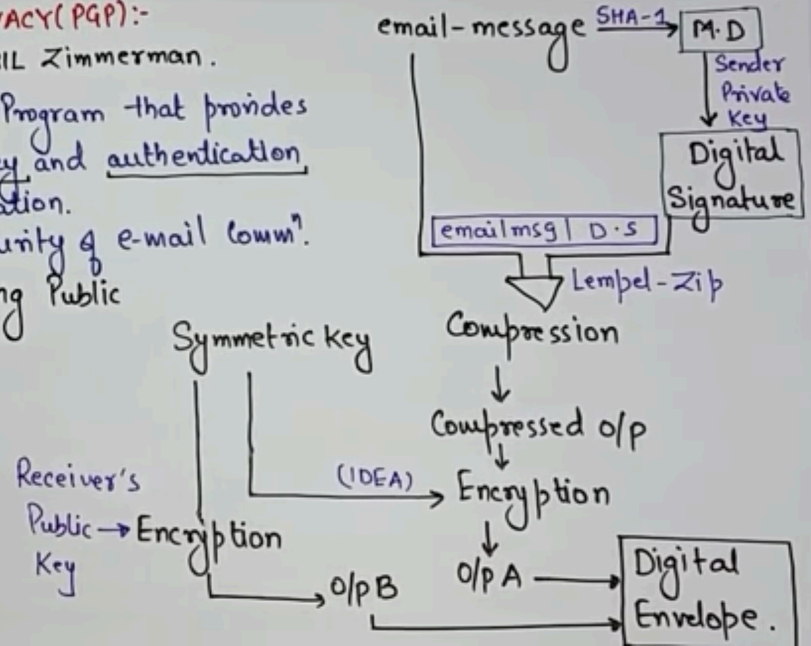
PRETTY GOOD PRIVACY (PGP):-

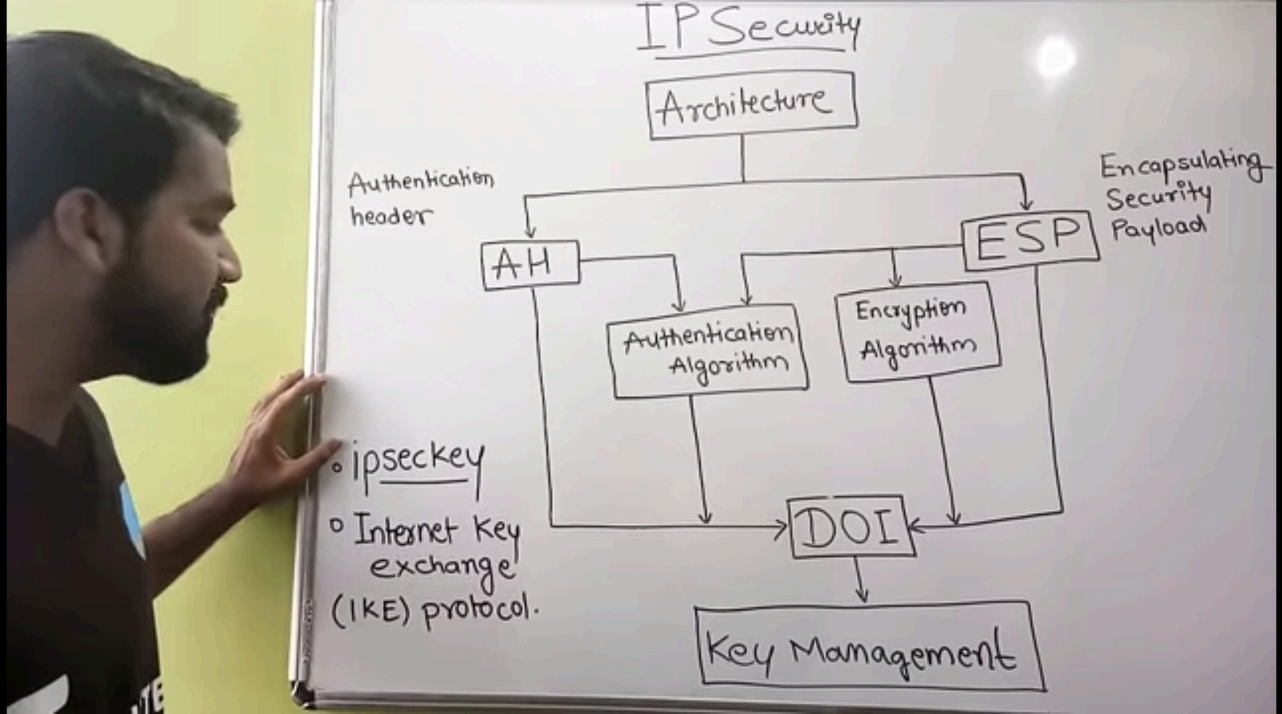
Father of PGP = PHIL Zimmerman.

It is an encryption Program that provides cryptographic privacy and authentication for data communication.

↳ Increases Security of e-mail comm^n.

PGP WORKING: using Public and Private Key Cryptography.




IP Security
Architecture
Authentication header
Encapsulating Security Payload
AH
ESP
Authentication Algorithm
Encryption Algorithm
DOI
Key Management
ipseckey
Internet Key exchange (IKE) protocol.

Security Association

1) Security Parameter Index
2) Security Protocol Identifier (AH/ESP)
3) Sequence number Counter (0 to $2^{32}-1$)
4) AH Information.
5) ESP Information.
6) Life time of SA
7) IPSec Protocol mode
   - Transport Mode
   - Tunnel Mode

Transport Mode

- Payload is encryted but not IP header

H	P

IP header	IPsec Header	Payload

AH
ESP

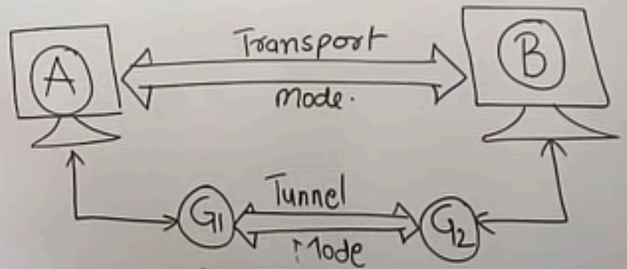
Encrypted.

Tunnel Mode

- Payload as well as IP header are encrypted.

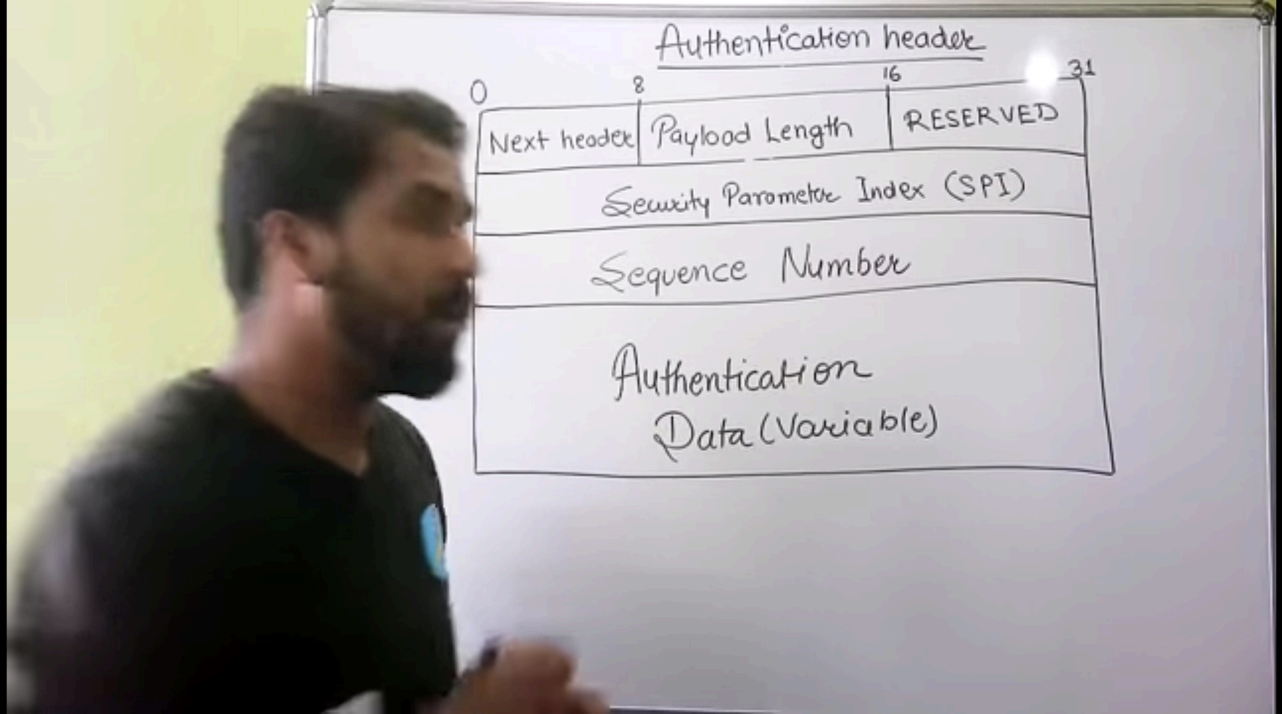
New IP Header	IPsec Header	IP header	Payload

Encrypted



Companies which hire from India for these roles :-

- ✓ Alpha Grep
- ✓ Tower research Capital
- ✓ Graviton Research
- ✓ NK Securities
- ✓ Wolved Quant
- ✓ Quadeye.


Authentication header
0
8
16
31
Next header
Payload Length
RESERVED
Security Parameter Index (SPI)
Sequence Number
Authentication Data (Variable)

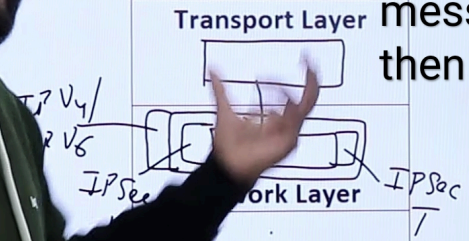
IP security (IPSec)

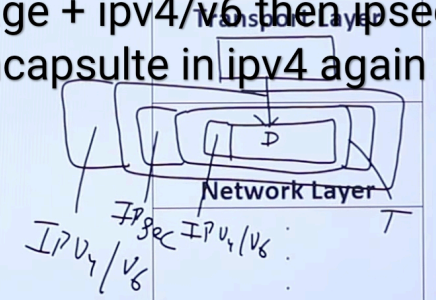
- IETF Standard
- Network layer protocol(Used both by IPv4 & IPv6)
- Uses of IP Security
  1. Confidentiality
  2. Authentication/Integrity
  3. Replay Attack Protection
- Collection of Protocols
  1. Encapsulating Security Payload (ESP)
  2. Authentication Header (AH)
  3. Internet Key Exchange (IKE)
- Two Modes of Operation(Transport Mode & Tunnel Mode)

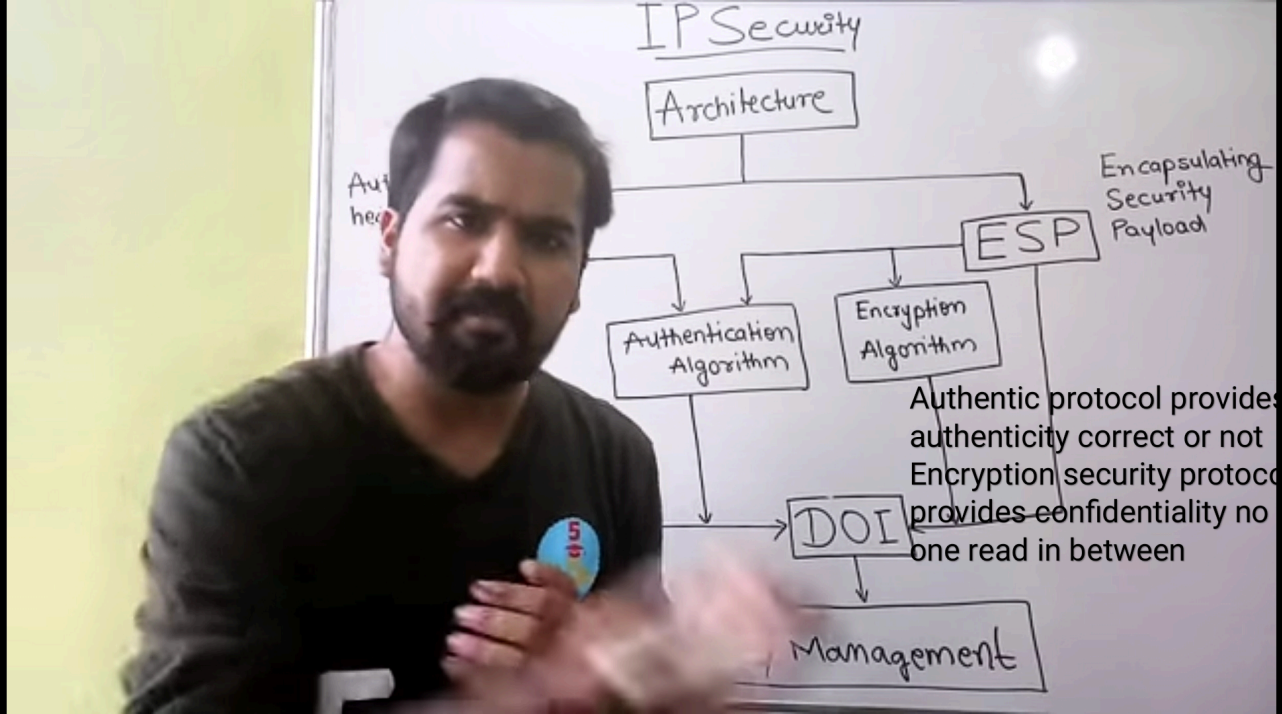
Transport Mode vs Tunnel Mode

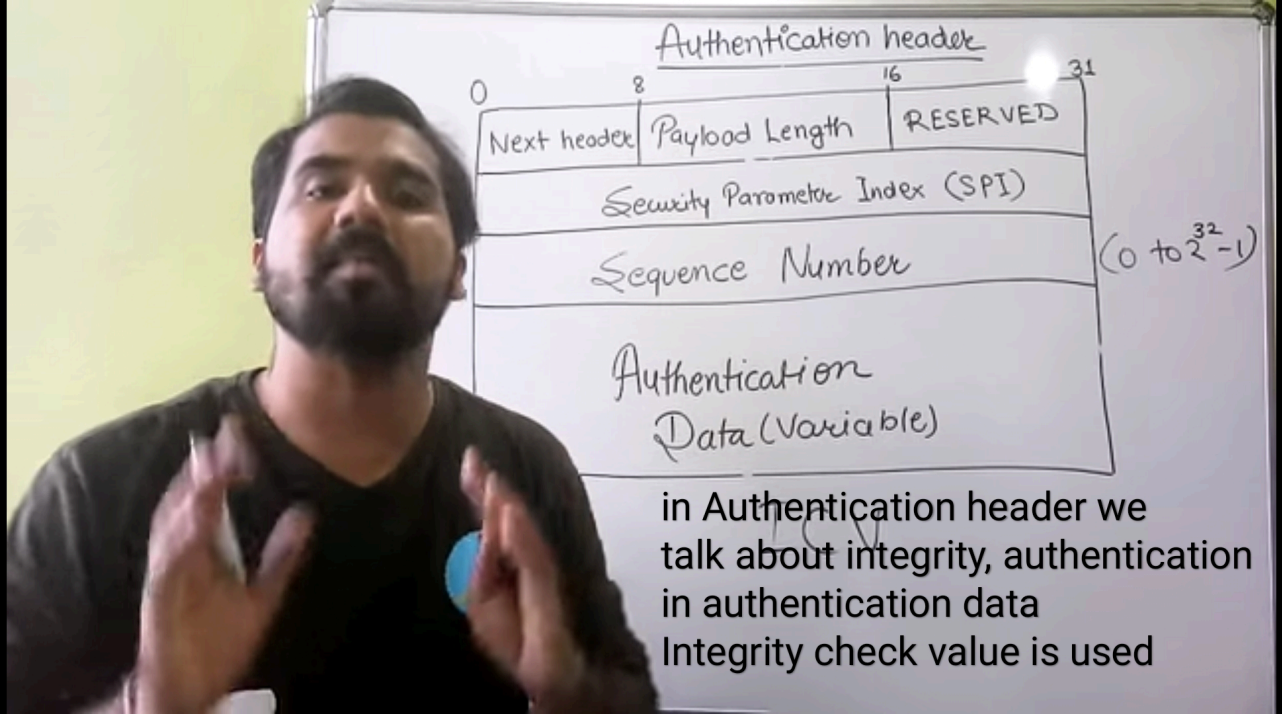
Transport mode :- end to end message + ip sec then + ipv4/v6

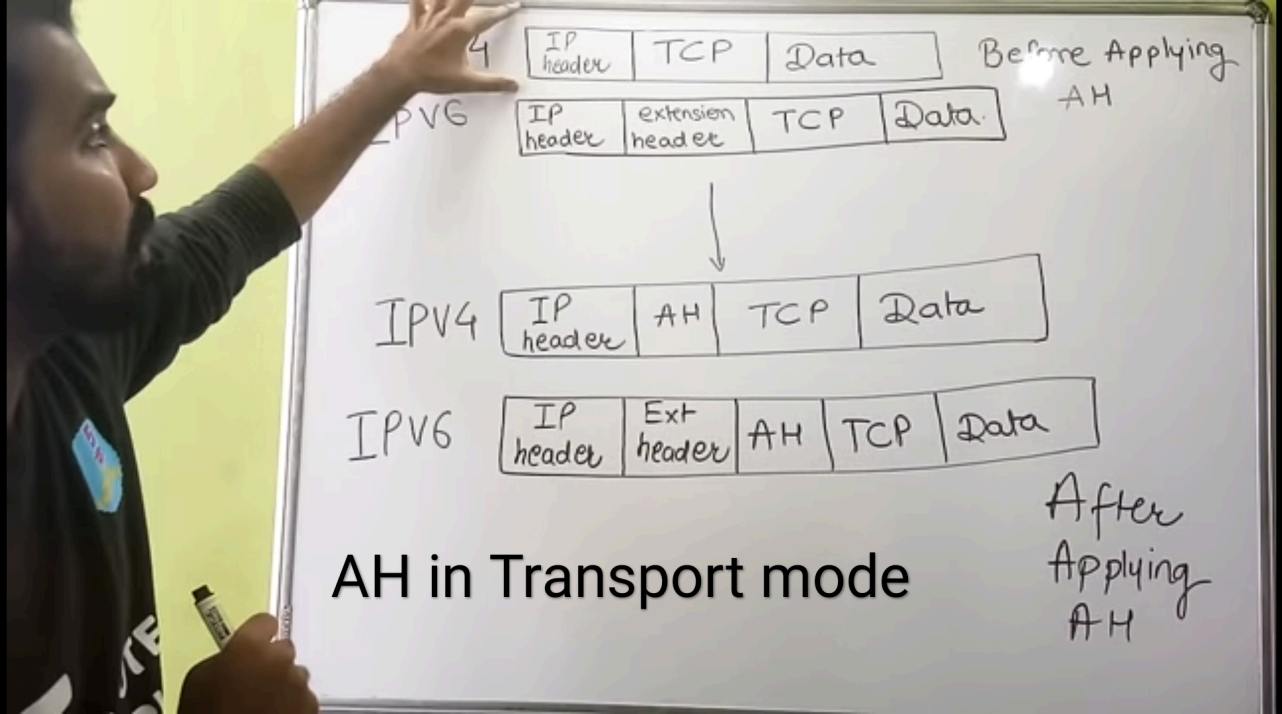
Tunnel mode :- Route to router message + ipv4/v6 then ipsec then incapsulte in ipv4 again

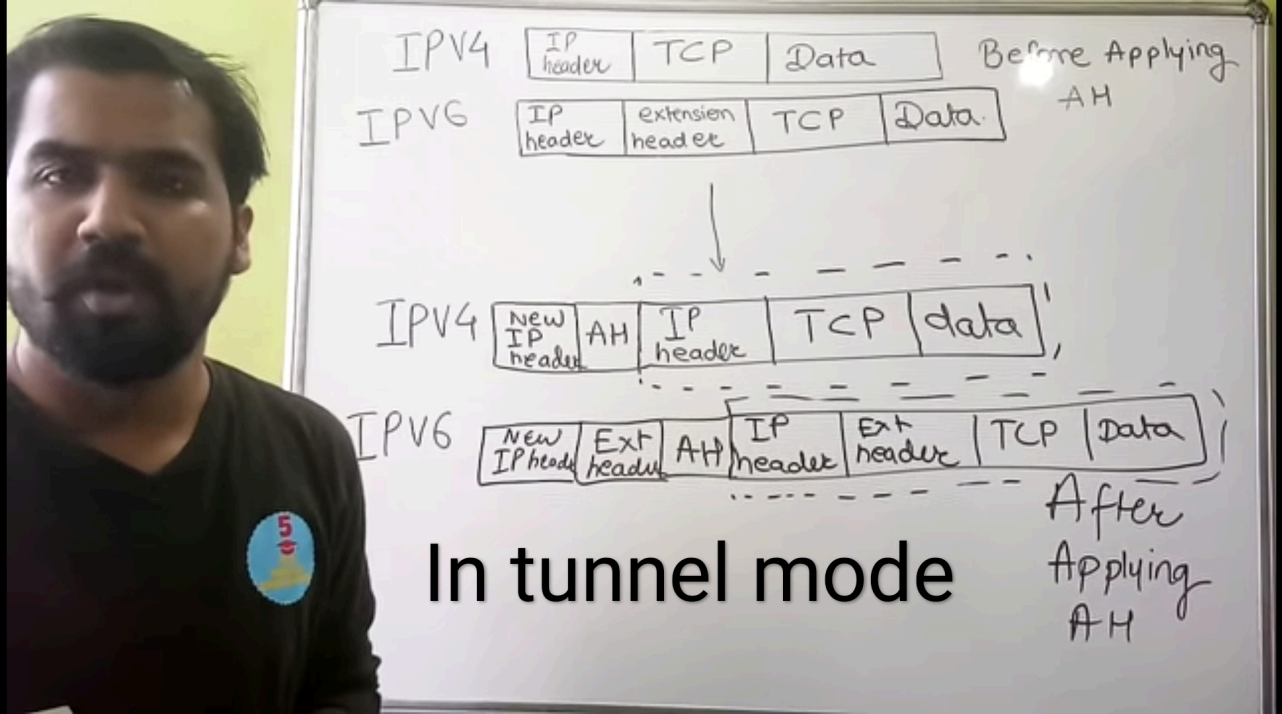


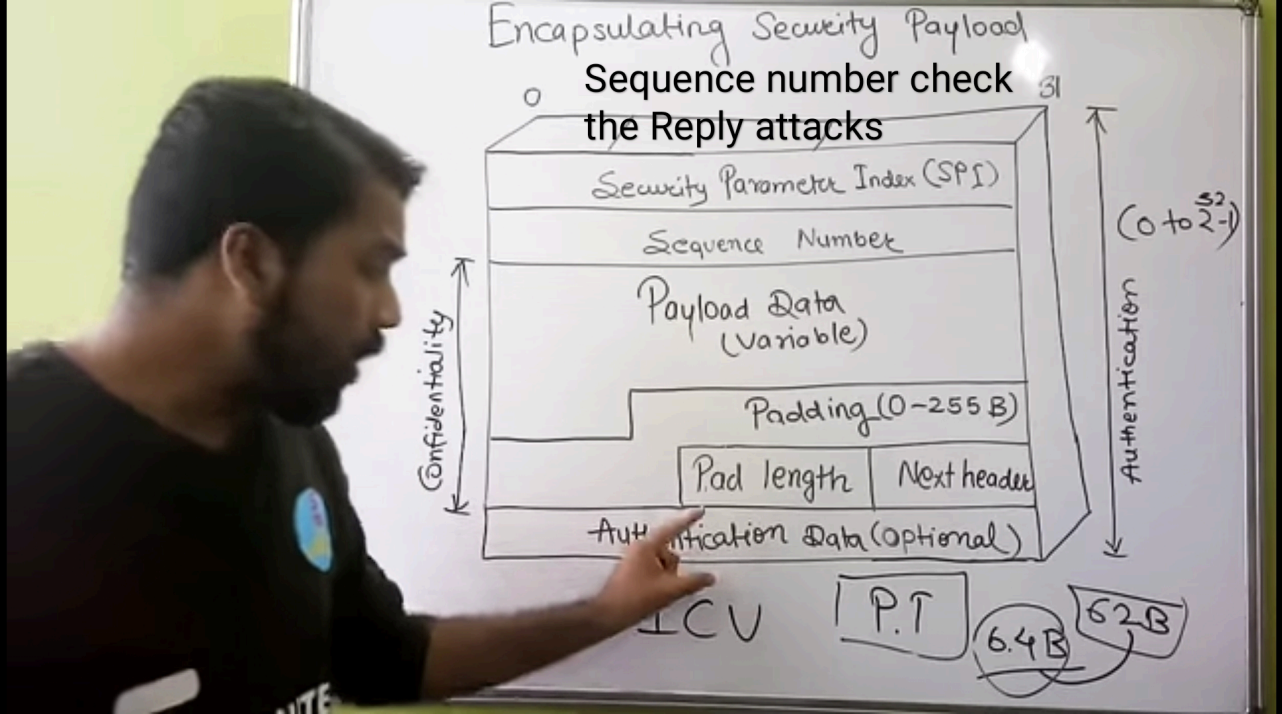


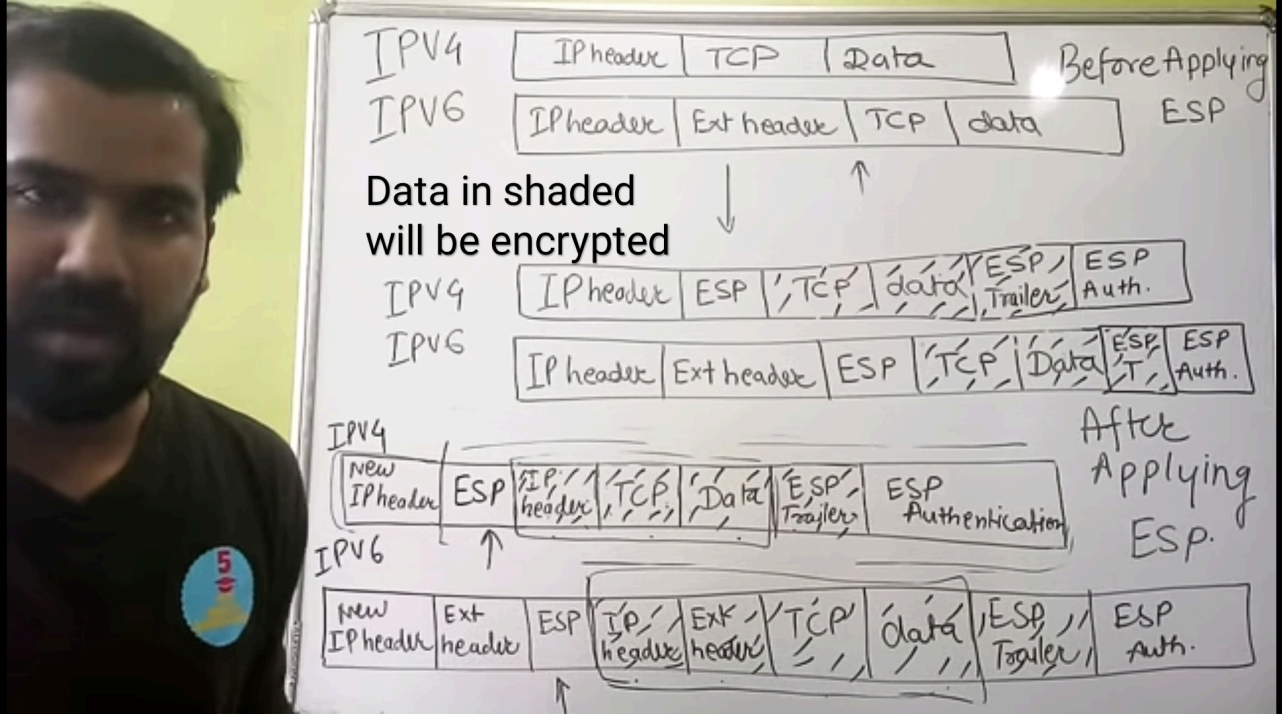

IP Security
Architecture
Encapsulating Security Payload
ESP
Authentication Algorithm
Encryption Algorithm
Authentic protocol provides
authenticity correct or not
Encryption security protoco
provides confidentiality no
one read in between
DOI
Management

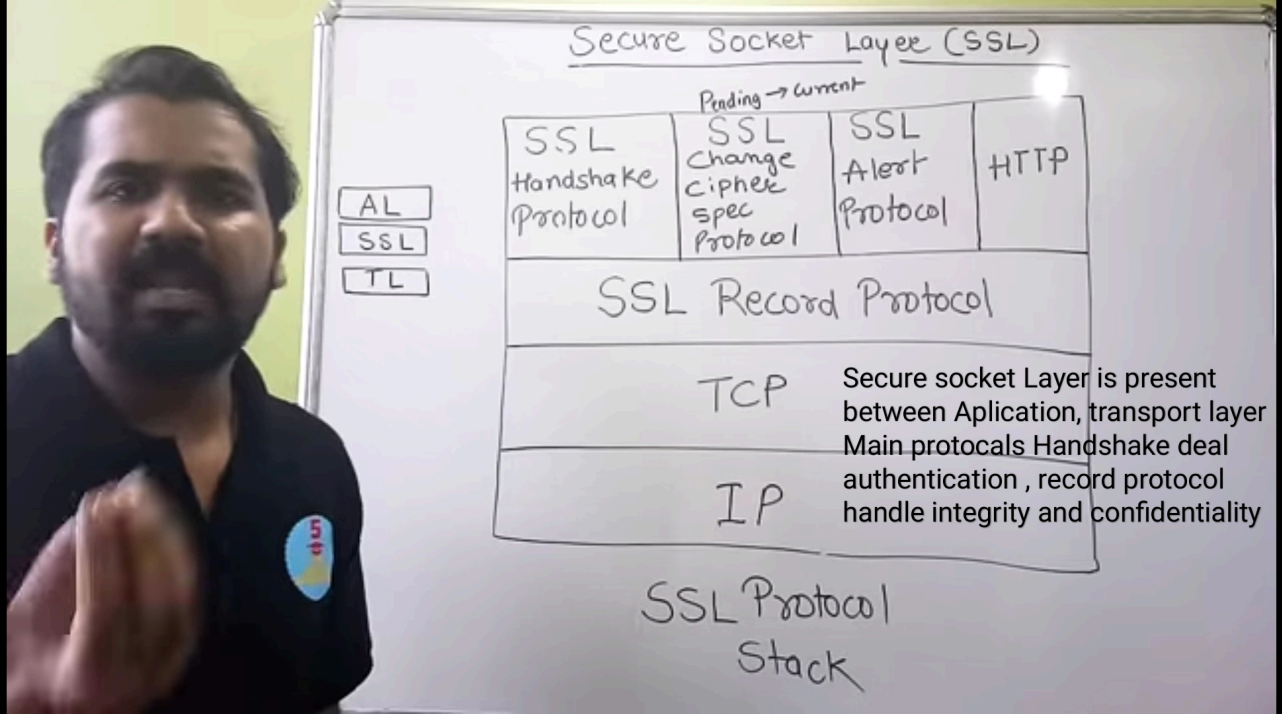

Authentication header
0
8
16
31
Next header
Payload Length
RESERVED
Security Parameter Index (SPI)
Sequence Number
(0 to 2^32 - 1)
Authentication Data (Variable)
in Authentication header we talk about integrity, authentication in authentication data Integrity check value is used


IP header
TCP
Data
Before Applying AH
IPV6
IP header
extension header
TCP
Data
IPV4
IP header
AH
TCP
Data
IPV6
IP header
Ext header
AH
TCP
Data
After Applying AH
AH in Transport mode

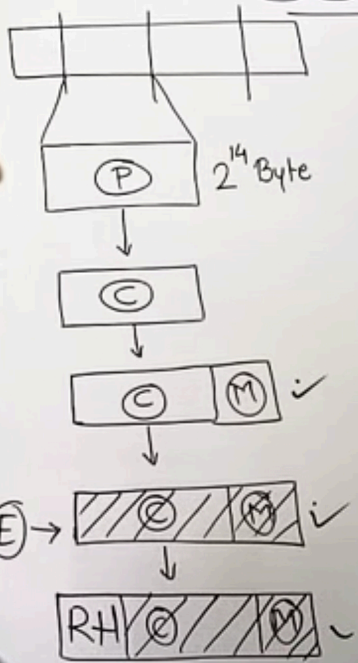

IPV4
IP header
TCP
Data
Before Applying AH
IPV6
IP header
extension header
TCP
Data
IPV4
New IP header
AH
IP header
TCP
data
IPV6
New IP header
Ext header
AH
IP header
Ext header
TCP
Data
After Applying AH
In tunnel mode

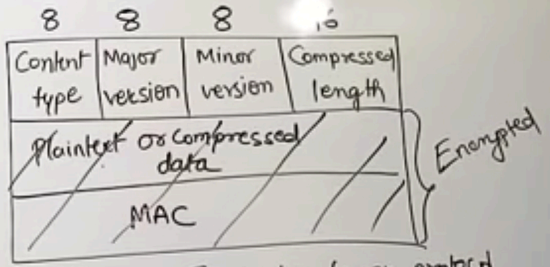

Encapsulating Security Payload
Sequence number check
the Reply attacks
0
31
Security Parameter Index (SPI)
Sequence Number
Payload Data
(Variable)
Padding (0-255 B)
Pad length
Next header
Authentication Data (optional)
Confidentiality
Authentication
(0 to 2^32 - 1)
ICV
P.T
6.4B
52B


IPV4
IP header
TCP
Data
Before Applying ESP
IPV6
IP header
Ext header
TCP
data
Data in shaded will be encrypted
IPV4
IP header
ESP
TCP
data
ESP Trailer
ESP Auth.
IPV6
IP header
Ext header
ESP
TCP
Data
ESP T.
ESP Auth.
IPV4
new IP header
ESP
IP header
TCP
Data
ESP Trailer
ESP Authentication
After Applying Esp.
IPV6
new IP header
Ext header
ESP
IP header
Ext header
TCP
data
ESP Trailer
ESP Auth.


Secure Socket Layee (SSL)
Pending → current
SSL Handshake Protocol
SSL Change cipher spec Protocol
SSL Alert Protocol
HTTP
SSL Record Protocol
TCP
IP
AL
SSL
TL
SSL Protocol Stack
Secure socket Layer is present between Aplication, transport layer
Main protocals Handshake deal authentication , record protocol handle integrity and confidentiality

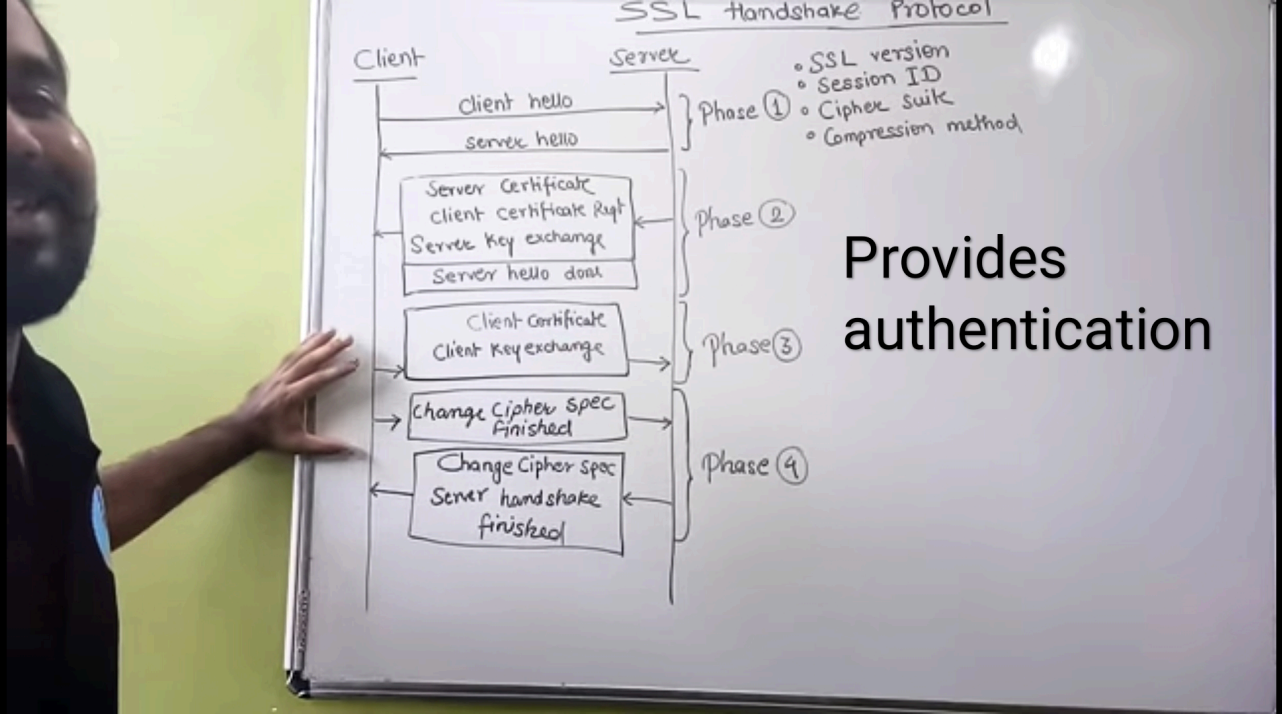
SSL Record Protocol



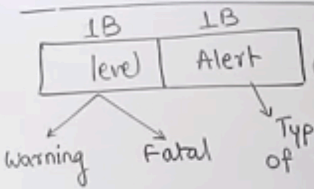


- Content type: The higher layer protocol used to process the enclosed fragment.
- Major version: For SSLv3 → value is '3'
- Minor version: value is '0'
- Compressed length: The length of compressed fragment in bytes.

from p to c compression must be lossless or optional


SSL Handshake Protocol
Client
Server
Client hello
Server hello
Phase 1
SSL version
Session ID
Cipher suite
Compression method
Server Certificate
Client certificate Rqt
Server Key exchange
Server hello done
Phase 2
Client Certificate
Client Key exchange
Phase 3
Change Cipher Spec
Finished
Change Cipher Spec
Server handshake finished
Phase 4
Provides authentication

SSL Alert Protocol



Alert msg : Description

- Close_notify → No more message sender
- Unexpected_message → Incorrect message received.
- bad_record_mac → Wrong mac received.
- bad_certificate → Received a corrupted certificate
- Certificate expired

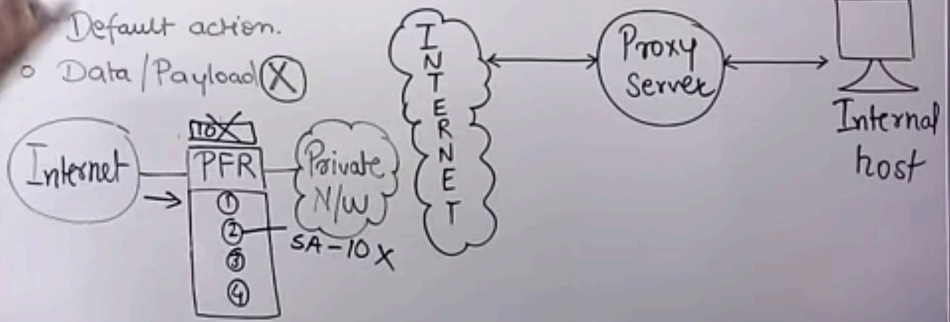
FIREWALL TYPES

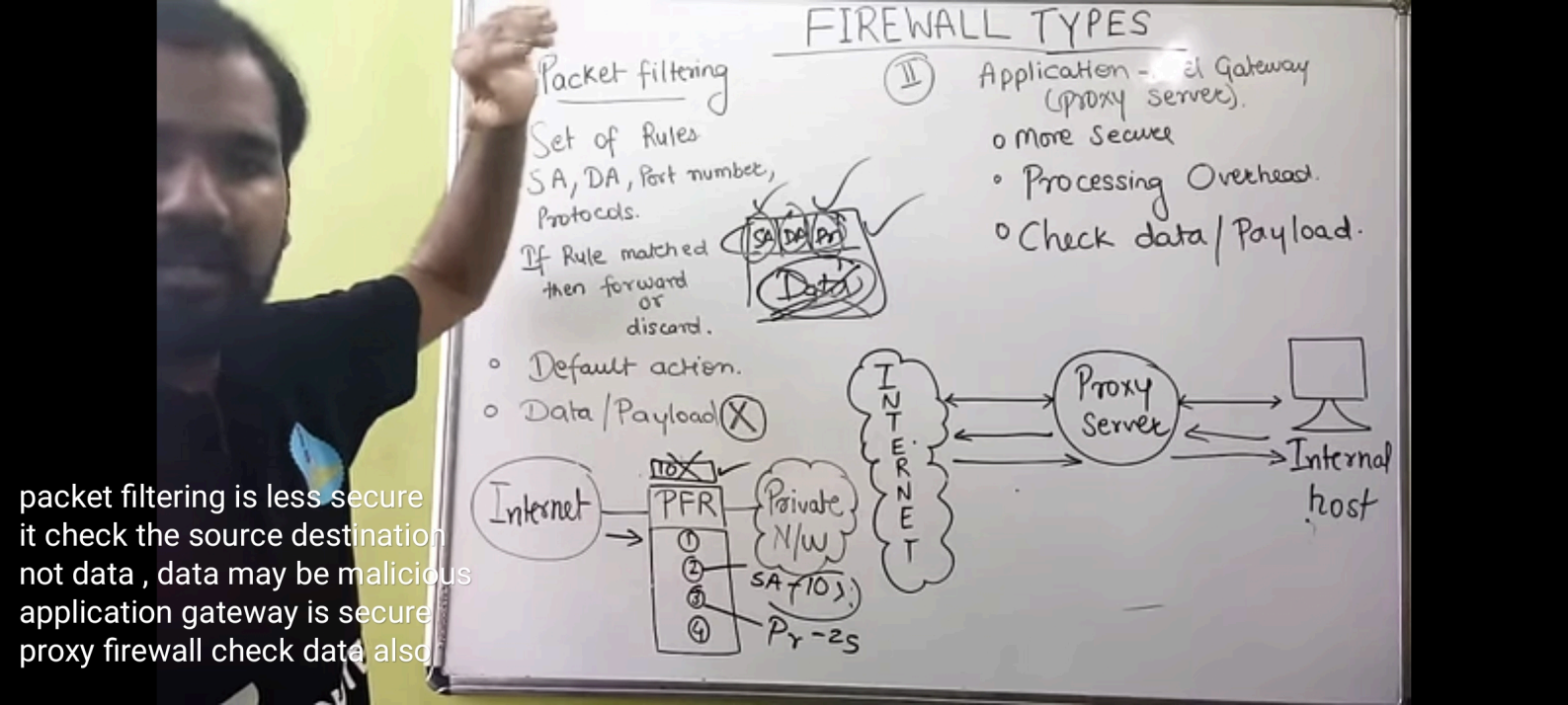
(I) Packet filtering

- Set of Rules
- SA, DA, Port number, Protocols.
- If Rule matched then forward or discard.
- Default action.
- Data / Payload (X)

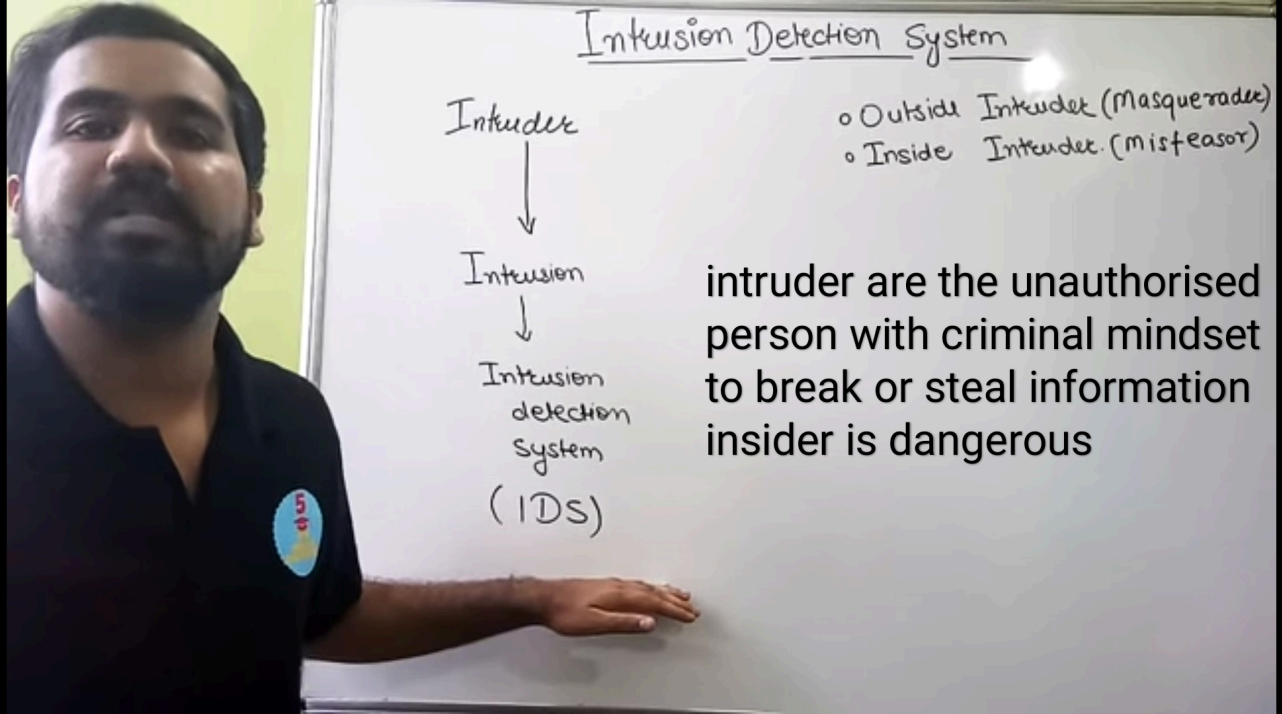
(II) Application - ~~Level~~ Gateway (Proxy Server).

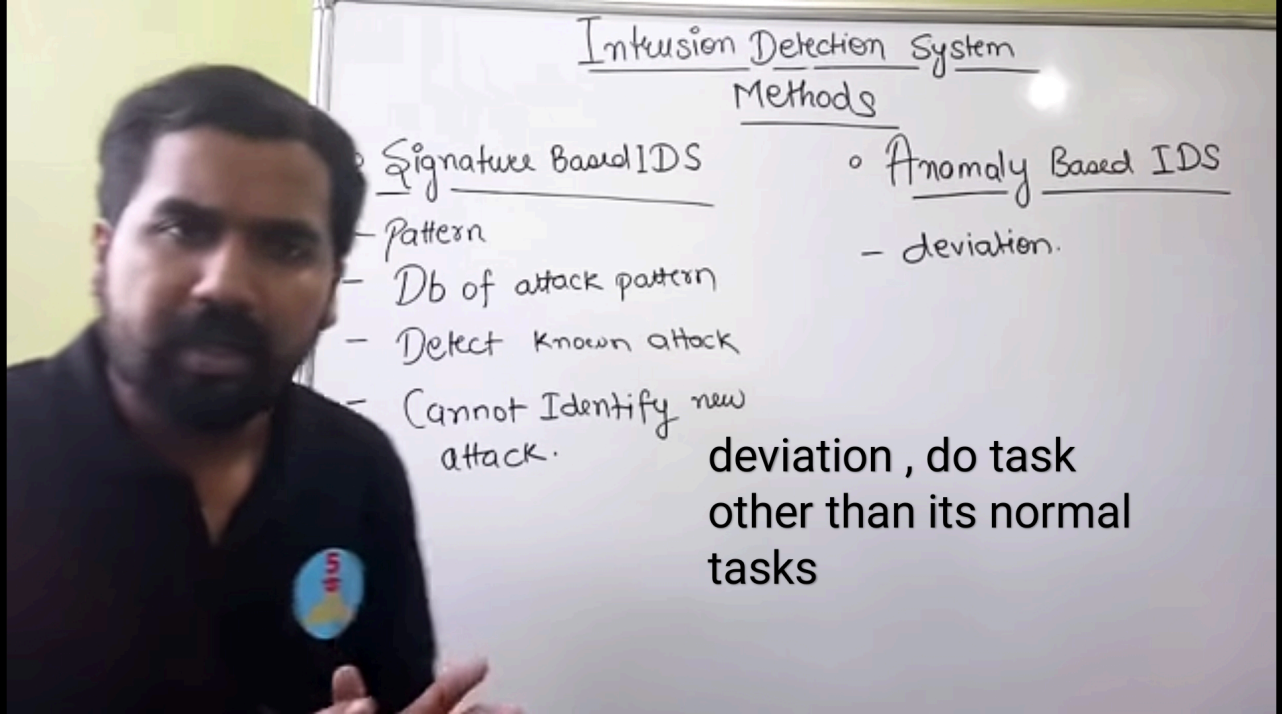
- More Secure
- Processing Overhead.
- Check data / Payload.

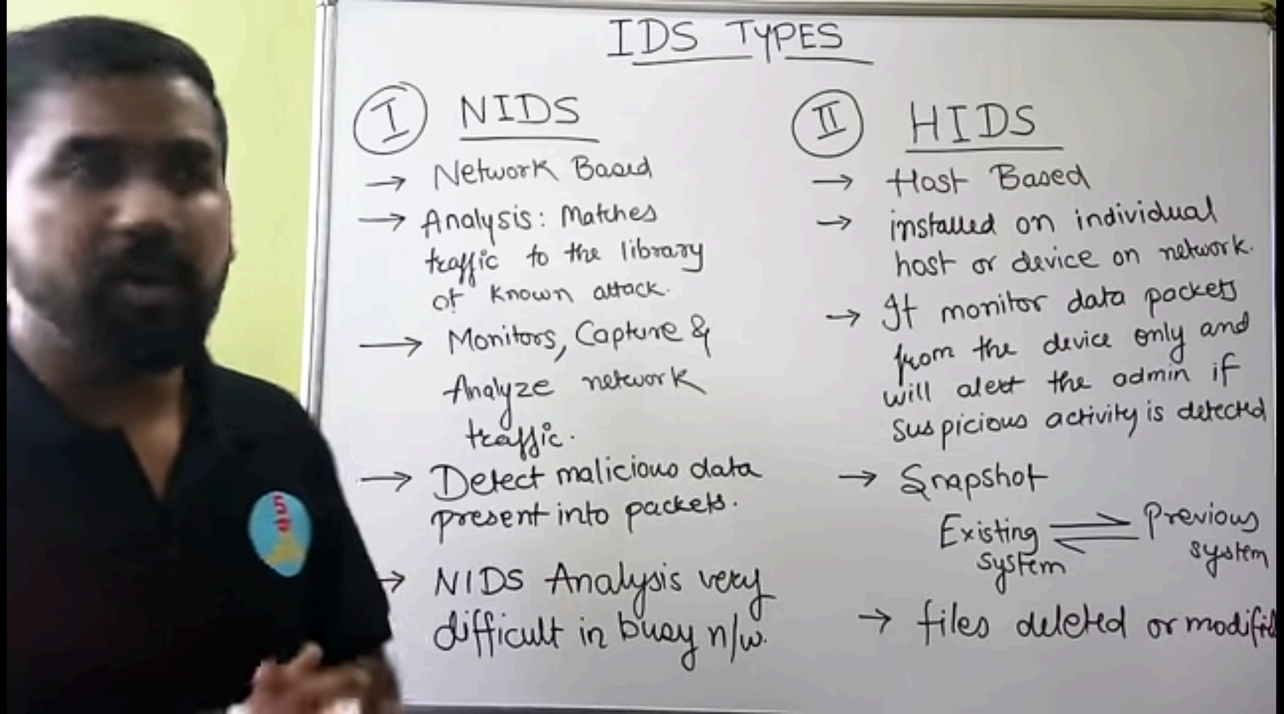




packet filtering is less secure
it check the source destination
not data , data may be malicious
application gateway is secure
proxy firewall check data also


Intrusion Detection System
Intruder
Intrusion
Intrusion detection System
(IDS)
Outside Intruder (Masquerader)
Inside Intruder (misfeasor)
intruder are the unauthorised person with criminal mindset to break or steal information
insider is dangerous


Intrusion Detection System
Methods
Signature Based IDS
- Pattern
- Db of attack pattern
- Detect known attack
- Cannot Identify new attack.
Anomaly Based IDS
- deviation.
deviation , do task other than its normal tasks


IDS TYPES
I NIDS
→ Network Based
→ Analysis: Matches traffic to the library of known attack.
→ Monitors, Capture & Analyze network traffic.
→ Detect malicious data present into packets.
→ NIDS Analysis very difficult in busy n/w.
II HIDS
→ Host Based
→ installed on individual host or device on network.
→ It monitor data packets from the device only and will alert the admin if suspicious activity is detected
→ Snapshot
Existing system ⇌ Previous system
→ files deleted or modifi