Name: Binod Kumar
Roll no: 23203006
Class: M.Tech (CSE)
Semester: IInd
Subject: Cyber Forensics
Assignment: 01

P.1) The IPsec architecture document states that when two transport mode SAs are bundled to allow both AH and ESP protocol on the same end-to-end flow, only one ordering of security protocol seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption?

Ans:

There are following two reason to perform ESP protocol before the AH protocol.

i) To prevent data leak

- If AH is performed before ESP, the data would be authenticated before being encrypted, which could potential leak information about the data. ie exposing it to potential eavesdropping.
- Since ESP provides confidentiality by encrypting the payload, while AH provides data integrity and authentication.

ii) Efficiency:

Since ESP encrypts the payload data, applying it first reduces the amount of data the AH algorithm needs to hash. This can improve processing efficiency, especially for large payloads.

5.2) What parameters identify an SA and what parameters characterize the nature of a particular SA?

Ans:

Security Association is identified by 3 parameters

i) Destination IP address:
This specifies the IP address of the recipient involved in the secure communication.

ii) Security protocol:
This identifies the type of security protocol used such as ESP or AH.

iii) Security parameter index (SPI):
This is a unique identifier assigned to the SA by the sender. It helps differentiate multiple SAs on the same device.

Now,
There are following parameters that characterize the nature of a particular SA.

i) Key length: The length of the encryption key used to secure the communication.

ii) Lifetime: The duration for which the SA is valid.

iii) Encryption Algorithm: such as AES, DES, 3DES.

iv) Authentication Method: This method used to authenticate the parties.

v) Perfect Forward Secrecy: This ensure that even if the encryption key is compromised, past communications remain secure.

vi) Quality of service (QoS):

The level of service that is provided by the security protocol, such as guaranteed bandwidth, low latency or high availability.

vi) Replay Detection:

Whether or not the security protocol provides protection against replay attacks, which is when an attacker intercepts and resends a message to try to gain access to the communication.

vii) Anti-Replay Window:

The length of time that the receiver will consider messages valid, after which they will be discarded to protect against replay attack.

Q.3) What is the difference between a TLS connection and a TLS session?

Ans:

A connection represents the communication link, while a session encapsulates the user-specific context and ongoing activities within that connection.

TLS connection	TLS session
i) A short-lived, point-to-point data transfer channel established between a client and a server.	i) A TLS session represents a longer-lived context or state maintained between a client and a server across multiple connections.
ii) It encompasses the entire process of negotiating and setting up the secure connection including the handshake, key-exchange, encryption & authentication;	ii) When a TLS connection is established, it can optionally be associated with a TLS session.

Q.4) List and briefly define the parameters that define a TLS session state and a TLS session connection.

Ans.

There are following parameters to define TLS session state.

i) Session ID: A unique identifier generated during the handshake to reference this specific session.

ii) Cipher suit: A combination of encryption, hash and key exchange algorithms used to secure the communication between the client and server.

iii) Master secret:

A secrete key generated by both the client and server during the handshake that is used to derive session keys for encryption and decryption.

iv) Compression method:

A method used to compress the data exchanged between the client and server.

v) Peer certificates:

Digital certificates used to authenticate the identities of the client and server.

vi) Is resumable:

A yes-no flag that allows new connections in an old session.

TLS session connection parameters.

i) **Client and server Random:**
Random values generated by each party during the handshake to create unpredictable session keys.

ii) **Read sequence Number:**
The next expected sequence number for incoming data on this connection.

iii) **Write sequence Number:**
The next sequence number to be used for outgoing data on this connection.

iv) **Connection-specific keys:**
Encryption keys derived from the master secret and random values, used for encrypting and decrypting data during this connection.

Q.5.) Two users A & B decide to use Diffie-Hellman key exchange technique a common prime $p = 71$ and a primitive root $g = 7$.

a) If user A has private key $X_A = 5$, what is A's public key Y_A?

Soln:

Public key, $Y_A = g^{X_A} \bmod p = 7^5 \bmod 71$

$= 16,807 \bmod 71$

$= 51$

$7^1 \bmod 71 = 7$

$7^2 \bmod 71 = 49$

$\therefore 7^5 \bmod 71 = (7^2 \times 7^2 \times 7^1) \bmod 71$

$= 343 \bmod 71$

5.b) If user B has private key $x_B = 12$, what is B's public key Y_B?

Soln:

Public key $Y_B = g^{x_B} \bmod P$

$= 7^{12} \bmod 71$

$= 4$

$7^1 \Rightarrow 7^1 \bmod 71 = 71$

$7^2 \Rightarrow 49 \bmod 71 = 71$

$7^3 \Rightarrow 7^3 \bmod 71$

$343 \bmod 71 = 59$

$7^4 \bmod 71 = (7^3 * 7^1) \bmod 71$

$= (59 \times 7) \bmod 71$

$= 413 \bmod 71$

$= 58$

$\therefore 7^{12} = (7^4 \times 7^4 \times 7^4) \bmod 71$

$= (58 \times 58 \times 58) \bmod 71$

$= 195,112 \bmod 71$

$= 4$

5.c) What is the shared secred key between A and B?

Soln:

Secrete key $= (Y_B)^{x_A} \bmod P$

$= 4^5 \bmod 71$

$= 1024 \bmod 71$

$= 30$

Both A and B will generate same shared secret key.

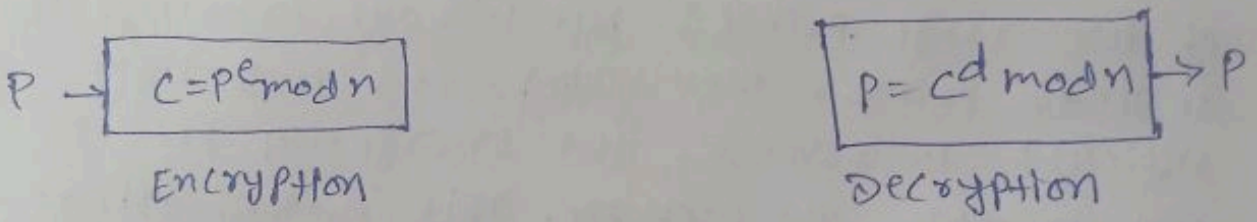
Q6) Briefly explain the idea behind the RSA cryptosystem.

1) What is the one-way function in this system?
2) What is the trapdoor in this system?
3) Describe the security of this system?

Ans:

The RSA cryptosystem is widely used public-key encryption algorithm that relies on the mathematical properties of prime numbers.

- RSA stands for (Rivest-Shamir-Adelman).



i) Select two large primes p & q such that $p \neq q$
ii) $n = p \times q$
iii) $\phi(n) \leftarrow (p-1) * (q-1)$
iv) Select e such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$.
v) $d = e^{-1} \bmod \phi(n)$
vi) public key = (e, n)
vii) private key : d
viii) plaintext : P
viii) ciphertext : C

One-way function

- The core RSA security relies on the one-way function of factoring large prime numbers. It is easy to multiply to large prime numbers together to get a very large composite number.
- However, reversing this process - factoring a large composite number back to its prime factors. It becomes computationally infeasible for sufficiently large numbers.

Trapdoor:

The trapdoor in RSA comes from the way the public and private keys are generated. These keys are mathematically linked through the product of two large primes, but without knowing the original primes themselves, it's incredibly difficult to reverse the encryption process and decrypt the message. This mathematical relationship between keys acts as the trapdoor.

Security:

- The security of RSA hinges on the difficulty of factoring large number (prime). As long as factoring these numbers remains computationally impractical, the system is considered secure.
- RSA security is also dependent on proper key management practices and the randomness of generated keys.

4-) Alice uses Bob's RSA public key (e=7, n=143) to send the plaintext P=8 encrypted as ciphertext C=57. Show how Eve can use the chosen ciphertext attack if she has access to Bob's computer to find the plaintext.

Ans:

- Since Eve knows the public key (e=7, n=143) and uses encryption process $C = P^e \bmod n$.
- She choose a related ciphertext C', mathematically linked to the original ciphertext C=57.
- A common approach, Eve can try to find the private exponent d using different techniques but for this chosen ciphertext attack, she can utilize the fact that e is small. (In this case e=7).
- To decrypt the ciphertext C, Eve can perform a brute-force search for the private exponent d by

$$C^d \equiv P \bmod n$$

$57^1 \bmod 143 = 57$

$57^2 \bmod 143 = 3249 \bmod 143 = 8$, which matches the plaintext P.

So, Eve has found the plaintext P=8 by trying d=2.