CS4331/CS5342 Network Security

Homework 3

Q.1. How many ways to achieve key distribution? (6.5 points)

Ans:

- A key could be selected by A and physically delivered to B.
- A third party could select the key and physically deliver it to A and B.
- If A and B have previously and recently used a key, one party could transmit the new key to the other, using the old key to encrypt the new key.
- If A and B each have an encrypted connection to a third party, C, C could deliver a key on the encrypted links to A and B.

Q.2. What are the requirements of many-to-many authentication? (8.5 points)

Ans:

1. Security:

- Protection against attacks by eavesdroppers and malicious users.

2. Transparency:

- Users should not notice the authentication process.
- Entering passwords is rare.

3. Scalability:

- Handles large numbers of users and servers.

Q.3. What are advantages and weaknesses of this protocol? (8.5 points)

Ans:

1. Steps:

- C → AS: ￼.
- AS → C: Ticket = ￼.
- C → V: ￼.

2. Advantages:

- Client and malicious attacker cannot alter ￼ (impersonate) or ￼ (change of address).
- Server ￼ can verify the user is authenticated through ￼.
- Guarantees the ticket is valid only if transmitted by the requesting client.

3. Weaknesses:

- Password is transmitted openly and frequently.

Q.4. What are advantages and weaknesses of secure authentication? (8.5 points)

Ans:

1. Steps:

- Once per user logon session:
- (1) C → AS: ￼.
- (2) AS → C: ￼.
- Once per type of service:
- (3) C → TGS: ￼.
- (4) TGS → C: ￼.
- Once per service session:
- (5) C → V: ￼.

2. Advantages:

- No password transmitted in plaintext.
- Ticket is reusable. Timestamp prevents reuse by attackers.

3. Weaknesses:

- Ticket Hijacking:
- Malicious users may steal a service ticket of another user on the same workstation.
- Network address verification does not help.
- No Server Authentication:
- Attackers may misconfigure the network to redirect users to a malicious server (man-in-the-middle attack).
- Servers must prove their identity to users.

Solution: Use session keys.

Q.8. What are the characteristics of the D-H key exchange? (8.5 points)

Ans:

1. No third party involved.
2. A common shared key (￼) is established.
3. The common shared key is symmetric.

Q.9. Describe D-H key exchange protocol with the help of a diagram. (8.5 points)

Ans:

- Alice and Bob share a prime ￼ and a primitive root ￼.
- Alice generates a private key ￼, calculates a public key ￼, and shares ￼ with Bob.
- Bob generates a private key ￼, calculates a public key ￼, and shares ￼ with Alice.
- Alice calculates the shared secret key ￼.
- Bob calculates the shared secret key ￼.

Q.10. What are the assumptions in the D-H key exchange protocol? (8.5 points)

Ans:

1. Discrete Logarithm Problem:

- Given ￼, it is computationally hard to find ￼.

2. Diffie-Hellman Assumption:

- No polynomial-time algorithm can compute ￼.

Q.11. What attack does D-H key exchange suffer? (8.5 points)

Ans:

1. David can alter messages, block messages, and send their own messages.
2. DH is not secure against MITM attacks (David can perform DH exchanges with both sides).

Q.12. Consider a Diffie-Hellman key exchange scheme with a common prime ￼ and a primitive root ￼. If User A has the public key ￼, and User B has the private key ￼, what is the shared secret key ￼? (8.5 points)

Ans:

￼.