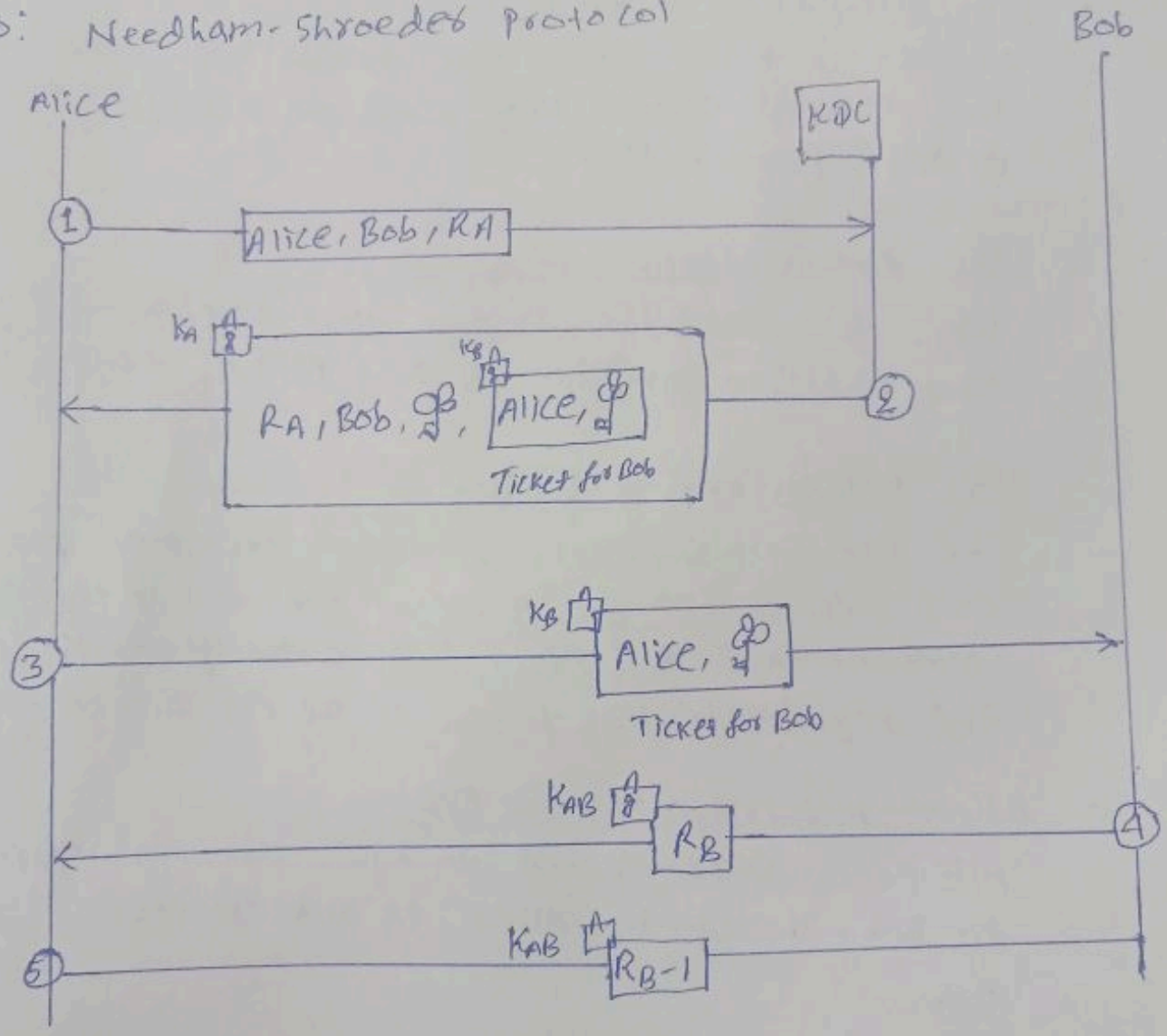
Name : Binod Kumar
Roll no : 23203006
Class : M-Tech CSE
Semester : 2nd
Subject : Network security
Assignment : 02

Q.1) In the Needham-Schroeder protocol, how is Alice authenticated by the KDC? How is Bob authenticated by the KDC? How is the KDC authenticated to Alice? How is the KDC authenticated to Bob?. How is Alice authenticated to Bob? How is Bob authenticated to Alice?

Ans: Needham-Shroeder protocol



- K_A : Encrypted with Alic-KDC secret key
- K_B : Encrypted with Bob KDC secret key
- K_{AB} : Encrypted with Alice-Bob session key
- : Session key b/w Alice and Bob
- R_A : Alice's nonce
- R_B : Bob's nonce
- KDC : Key-distribution center

Now.

- Alice Authentication by KDC
  - The KDC does not authenticate Alice in the traditional sense. It trusts Alice based on the shared secret key she uses to send the initial request.

- Bob authenticated by KDC:
  Similar to Alice, the KDC trusts Bob based on the shared secret key used to decrypt the message from Alice.

- KDC Authentication to Alice
  KDC is an authorized and well known entity. The whole assumption is that Alice trusts KDC.

- KDC Authentication to Bob
  The Needham-Shroeder protocol does not provide any mechanism for Alice or Bob to explicitly authenticate the KDC. They simply trust it's the legitimate KDC based on the Pre-shared keys.

- Alice Authentication to Bob
  Alice is authenticated to KDC. KDC is authenticated to Bob. Therefore, Alice is authenticated to Bob.

- Bob Authentication to Alice
  Since Bob is authenticated to KDC. KDC is authenticated to Alice. Therefore, Bob is authenticated to Alice.

Q.2) In the Diffie-Hellman Protocol, $g=7$, $P=23$, $x=3$ and $y=5$.

a. What is the value of the symmetric key?

b. What is the value of R_1 and R_2.

Soln:

Symmetric key, $K = g^{xy} \bmod P$

$K = 7^{3\times5} \bmod 23$

$K = 7^{15} \bmod 23$

$K = 14$

$7^1 \bmod 23 = 7$

$7^2 \bmod 23 = 3$

$\therefore 7^{15} = 7^2$

$7^4 \bmod 23 = (7^2 \times 7^2) \bmod 23$

$= (3\times3) \bmod 23$

$\therefore 7^4 \bmod 23 = 9$

$7^6 \bmod 23 = (7^4 \times 7^2) \bmod 23$

$= (9\times3) \bmod 23$

$7^6 \bmod 23 = 4$

$7^7 \bmod 23 = (7^6 \times 7^1) \bmod 23$

$= (4\times7) \bmod 23$

$= 5$

$\therefore 7^{15} \bmod 23 = (7^7 \times 7^7 \times 7^1) \bmod 23$

$= [(7^7 \bmod 23) * (7^7 \bmod 23) \times (7^1 \bmod 23)] \bmod 23$

$= (5 * 5 * 7) \bmod 23$

$= 175 \bmod 23$

$= 14.$

P: Prime nos

g: generator of order P-1

Now, $R_1 = g^x \bmod P$

$= 7^3 \bmod 23 = 21$

$R_2 = g^y \bmod P = 7^5 \bmod 23 = 17$

Q.3) List the duties of PKI.

Ans: Public-key infrastructure (PKI) is a model for creating, distributing and revoking certificate based on the X.509.

There are following duties of PKI.

i) Certificates issuing, renewal, and revocation.
These are duties defined in the X.509. Because the PKIX is based on X.509, it needs to handle all duties related to certificates.

ii) Keys storage and update.
A PKI should be a storage place for private keys of those members that need to hold their private keys somewhere safe. In addition, a PKI is responsible for updating these keys on members demands.

iii) Providing services to other protocols
For example, IPSec and TLS are relying on the services by a PKI

iv) Providing access control
A PKI can provide different levels of access to the information stored in its database.

For example, an organisation PKI may provide access to the whole database for the top management, but limited access for employees.

Q.4) In the Diffie-Hellman protocol, what happen if x and y have the same value, that is Alice and Bob have accidentally chosen the same number? Are R1 and R2 same? Do the session keys calculated by Alice and Bob have the same value? Use an example to prove your claims.

Ans: As we know $R_1 = g^x \bmod P$ & $R_2 = g^y \bmod P$

if $x = y$ then $R_1 = R_2$

ie Both R_1 and R_2 are same.

For key, $K = g^{xy} \bmod P$

$K = R_2^x \bmod P$, $K = R_1^y \bmod P$

Here, $x = y$ and $R_1 = R_2$.

So, Also K is the same.

Example: $P = 23$, $g = 7$, $x = 3$, $y = 3$

$R_1 = g^x \bmod P = 7^3 \bmod 23 = 21$

$R_2 = g^y \bmod P = 7^3 \bmod 23 = 21$

$K = R_2^x \bmod P = 21^3 \bmod 23 = 14$

$K = R_1^y \bmod P = 21^3 \bmod 23 = 14$

Q.5) Discuss the limitations of Diffie-Hellman key exchange algorithm.

Ans: It has following limitation

i) Lack of authentication procedure

ii) It is vulnerable to man-in-the middle attack

iii) Diffie Hellman can be used only for symmetric key exchange.

iv) As it is computationally intensive, it is expensive in terms of resources and CPU performance time.

v) Encryption of information can not be performed with the help of this algorithm.

vi) Digital signature can not be signed using Diffie-Hellman algorithm.

6 b) Define a nonce and its use in entity authentication

Ans: A 'nonce' is a random number specially used to prevent replay attacks during entity authentication

- Entity authentication is the process of verifying the identity of a user or device involved in a communication.
- Replay attacks exploit the fact that communication channels can be intercepted. An attacker might capture login information containing a username and password and they try to use that information later to impersonate the legitimate user.

Now, how nonces thwart replay attacks

1) Uniqueness: A true nonce is random value used only once. This make it unpredictable for an attacker to guess or reuse a capture nonce in a future attempt.

ii) Challenge-Response:

In a typical authentication protocol using nonces, one entity (server) sends a challenge containing a fresh nonce to other entity (client). The client incorporates this nonce into its response along with other authentication factors like a password.

iii) Verification:

The server verifies the response. If the nonce is valid ie has not been seen before, the server can be confident the message is fresh and not a replay of a previous interaction.

Q.7) For $P=569$, $q=683$ and $S=157$. Show three rounds of the Fiat-Shamir protocol by calculating the values and filling in the entries of a table.

Soln Given, two large prime P & q

where $P=569$ and $q=683$. And private key $S=157$.

$$\therefore n = P \times q = 569 \times 683 = 388,627$$

$$\therefore v = s^2 \bmod n = (157)^2 \bmod 388,627$$
$$= 24,649 \bmod 388,627$$

- public key $\therefore v = 24649$
- random number, r between 0 to $n-1$.
  r is also called commitment.
- Witness, $x = r^2 \bmod n$
- Challenge, c can be either 0 or 1.

S : Private key
v : Public key

Random no. or commitment ↓	Witness ↓	challenge ↓			
γ	$x = r^2 \bmod n$	c	$y = r s^c \bmod n$	$y^2 \bmod n$	$x v^c \bmod n$
203,122	130663	0	203122	130,663	130,663
153,871	292,873	1	379,260	366,513	366,513
377,295	345,180	1	210,881	247,049	247,049

Here, The values of last two column should be same if Alice is honest or has pre-guessed the value of c.

Q.8) In the Fiat-Shamir protocol, what is the probability that a dishonest claimant correctly responds to the challenge 15 times in a row?

Ans In the Fiat-Shamir protocol, a dishonest claimant can correctly responds to a Pr change with the probability of 1/2.

The probability that a dishonest claimant responds correctly 15 time is $1/2$

$$= (1/2)^{15}$$

$$= \frac{1}{32768}$$

$\simeq 0.0000305$, which is very small.

Q.9) How can a system prevent a guessing attack on a password? How can a bank prevent PIN guessing if someone has found or stolen a bank card and tries to use it?

Ans. Preventing guessing attacks on password. There are following some strategies

i) Encourage users to create strong passwords that are difficult to guess by requiring a minimum length & combination of uppercase, lowercase letters, numbers and special characters.

ii) Enforcing regular password changes.

iii) Implement account lockout mechanisms that temporarily lock user accounts after a certain number of failed login attempts. This prevents attackers from making unlimited ~~response~~ guesses.

iv) Implement rate limiting on login to prevent brute force attacks. This involves limiting the number of login attempts from a single IP address or user account within a specified time period.

v) Introduce CAPTCHA or challenge-response tests during the login process to ensure that the login attempts made by human and not by automated bots.

vi) Implement multi-factor authentication approach. Require users to authenticate using multiple factors such as password, biometrics (fingerprint, facial recognition) or hardware tokens.

Now,

There are following strategies regarding preventing PIN guessing for bank cards.

i) Similar to account lockout mechanism for passwords, banks can implement card lockout mechanism that deactivate the card after a certain number of incorrect PIN attempts.

ii) Some banks have started implementing dynamic card verification value (CVV) systems, where CVV changes periodically, making it useless for attackers who have stolen the card details but do not have the current CVV.

iii) Implement transaction monitoring systems that detect unusual or suspicious activity such as multiple failed PIN attempts and flag them for further investigation or block the transaction.

iv) Educating the customers about the importance of keeping their PIN confidential and not sharing it with anyone.

Q.10) Discuss the various attacks at the network layer with suitable examples.

Ans: Here are some common network layer attacks

1. Denial of service (DOS) Attacks

These attack aim to overwhelm a network or servers with traffic, making it unavailable to legitimate users.

- Ping flood: The attackers bombards the target with a massive amount of ping requests, overloading its resources and preventing it from responding to legitimate traffic.

- Smurf attack: A more malicious version of a ping flood. The attackers spoofs the source IP address of the ping requests to be the target's IP address. This floods the target with responses from other devices on the network taking it down.

2. Spoofing Attacks
These attacks involve impersonating a legitimate device on the network to intercept or manipulate data traffic.

- ARP Spoofing: The attacker sends fake address resolution protocol (ARP) message to a target device, tricking it into sending data packets to the attacker's machine instead of the intended recipient. This allows the attacker to eavesdrop on communication or redirect traffic.

- IP Spoofing: IP spoofing involves forging the source IP address of packets to disguise the identity of the sender.
Example; An attacker might spoof their IP address to impersonate a trusted entity, allowing them to bypass access controls or launch attack while appearing to originate from a different source.

3. Routing attack
These attacks manipulate how data packets are routed through the network.
DNS Spoofing: The attacker redirect the DNS requests to a malicious website by provide false information about a domain's IP address. This can trick users into unknowingly visiting a compromised site.

- Route Hijacking: The attacker diverts network traffic intended for a specific destination to a different location, allowing them to intercept data or launch further attacks.

4. Man-in-the-middle (MitM) attack:
These attacks position the attacker between two communicating devices, allowing them to eavesdrop on or tamper with the data exchange.

- IP Hijacking: The attacker exploits a weakness in a network connection to insert themselves into the communication flow between two devices. This allows them to steal data or inject malicious code.

- Session Hijacking: The attacker takes over an existing communication session between two devices. This can be done by stealing session cookies or exploiting vulnerabilities in network protocols.

5. ICMP Attacks
This attack exploit weakness in the ICMP Protocol to disrupt or degrade a network connectivity.
Example: ICMP flood attacks involve sending a large volume of ICMP Echo request packet to a target network or device, consuming its resources and potentially causing it to become unresponsive.

Q.11) Discuss the UDP storm attack in detail with real-time examples.

Ans: A UDP storm attack is a type of Denial-of-service (DOS) attack that leverages the UDP to overwhelm a target system with a massive volume of UDP packets.

Working of UDP storm

i) The attacker generates or spoofs a large volume of UDP packets, each containing a forged source IP address. These packet are sent to the target network at a high rate.

ii) The target network's resources such as bandwidth, CPU and memory become overwhelmed as it tries to process and respond to the flood of incoming UDP packets.

iii) The sheer volume of UDP packets consumes all available resources, causing legitimate traffic to be dropped or delayed. As a result, the targeted network or service becomes unavailable to legitimate users.

iv) In some cases, attackers may use amplification techniques to increase the volume of attack traffic. This involves exploiting servers or services that respond with larger packets than those initially sent by attacker, amplifying the impact of attack.

Real-time examples

Imagine you're streamer on a live gaming platform. You are engrossed in a competitive match, interacting with your audience. When a suddenly, your internet connection grinds to a halt. You see buffering, dropped frames and frustrated comments flooding your chat.

Behind the scenes, an attacker might be launching a UDP storm attack on the gaming platform's servers.

Example 2

Imagine a popular online store during a sale. A UDP storm attack could bombard the store's servers with millions of UDP packets per second. The servers, struggling to handle the onslaught, wouldn't be able to process legitimate customer requests, effectively taking down the online store and causing revenue loss.

Mitigating UDP storm attack

i) Traffic filtering
ii) Rate limiting
iii) UDP flood detection
iv) IP reputation filtering
v) Protocol Hardening