**CS1 – Assignment 2**

**Q1 - Briefly describe the five IEEE 802.11i phases of operation.**

802.11i is an amendment to the original IEEE 802.11 a security standard for secure authentication and data encryption for wireless networks that provides improved encryption for networks.

The five IEEE 802.11i phases of operation for wireless network security are:

Authentication: This is the first phase of IEEE 802.11i where the access point and client end point authenticate each other’s identities. There are two types of authentication methods – Pre-Shared key (PSK) and 802.1X/EAP. In PSK method, a shared key is used to authenticate access point and client end point whereas in 802.1X/EAP method it uses backend authentication. The different steps in this phase are connect to Authentication Server, Extensible authentication protocol exchange, and Secure Key Delivery.

Key Generation: Once the client end point and access points have authenticated each other, they generate session keys for encryption and decryption of data. Key Generation phase defines a four-way handshake protocol for key generation that involves exchanging messages between the client and access point to derive a Pairwise Master Key (PMK) and a Pairwise Transient Key (PTK)

Encryption – After the session keys in place, the client and access point now encrypt and decrypt the data using the Advanced Encryption Standard (AES) encryption algorithm. This standard provides different modes of operation for AES: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Temporal Key Integrity Protocol (TKIP).

Integrity - To avoid any data tampering and maintaining data integrity, IEEE 802.11i uses the Message Integrity Check (MIC) algorithm to produce a hash value of the data and add it to the encrypted message. The destination end point verify the MIC to make sure that the message has not been altered or tampered during transit.

Key Management – Final phase defines mechanisms for key management and rekeying to ensure the security of the wireless network over time. Key management involves generating new session keys periodically, while rekeying involves renegotiating session keys if they are compromised or leaked or old.

These phases work together to ensure that the wireless network is secure by using encryption, authentication, integrity and key management.

**Q2 - Write any 2 unlinkability attacks against 5G-AKA**

5G-AKA (Authentication and Key Agreement) is one of the security protocols mainly used in 5G networks to establish a secure communication link between the user and network. The protocol ensures the confidentiality and integrity of communication between the network and the device. Unlinkability attacks are a type of security threat that aims to break the anonymity of a user by linking their identity across different communication sessions. There are some unlinkability attacks that can compromise the privacy and integrity of the user. Here are two examples:

IMSI catchers:

An IMSI (International Mobile Subscriber Identity) catcher is a device that can intercept the IMSI of a mobile device. In the 5G-AKA protocol, the IMSI is a unique identifier that is assigned to a mobile device and is used by the network to authenticate the device and provide thes services. An attacker intercepts the IMSI of a device, so that they can use it to track the user's transactions, activities, location, and other sensitive data. This attack can compromise the unlinkability of the user, as the IMSI can be used to link the user's activities across different sessions. IMSI catchers are widely used by law enforcement agencies to track the location of a mobile device or to intercept communications.

Reauthentication Attack:

In this attack, an adversary can observe the authentication process between the user and the network and record the authentication parameters, such as the user's Identity Key (IK) and Authentication Token (AUTN). The attacker uses these parameters to impersonate the user and initiate a new authentication process, which cannot be distinguishable from the original authentication process. This attack breaks the unlinkability property of 5G-AKA, as the network cannot distinguish between the original user and the attacker.

**Q3 - In GSM,**

**(a) We assume that each subscriber has been assigned an IMSI (i. e. International Mobile Subscriber Identity), and this information is publicly known. If we want to provide a service to hide this information even during the initial connection (i.e. including the registration), suggest one solution to satisfy this requirement. You need to point out how and why this solution can protect IMSI. (no more than 30 words)**

By using temporary identifier called Temporary Mobile Subscriber Identity (TMSI), assigned by the VLR during the registrations. TMSI used for all subsequent communications and provides anonymity for the user.

**(b) Multiple SRESs and RANDs are stored at VLR for authentication purposes, where SRES=A3( Ki, RAND) and Ki is a pre-shared secret key between the mobile subscriber and HLR. SRES needs to be protected and used as evidence to collect a service fee. Since SRES is known by both mobile subscribers and VLR, repudiation cannot be resolved. If we want to establish a partially non-repudiation service between the mobile subscriber and VLR, suggest one solution to meet this requirement. (no more than 30 words)**

VLR can send a random number to subscriber, mobile subscriber can use SRES and the random number to generate response for identity. This provides partial non-repudiation as the response is unique.

**Q4 - In most wireless communications, there are 3 entities involved in connecting a call: Mobile Subscriber (MS), VLR, and HLR.**

**(a) Suggest a method that MS can protect its identity when MS roams into a new VLR region. (i.e. MS does not need to expose its real identity to the attacker when makes the first connection through VLR)**

Visitor Location Registers (VLR) corresponds to a temporary database that modifies and updates its entries whenever a new mobile subscriber joins a specific area under the HLR database. VLR helps HLR to reduce direct queries to HLR. One method for MS to protect its identity when roaming into a new VLR region is for the MS to use a temporary identity provided by the VLR instead of its real identity. In order to secure the mobile subscriber (MS), a Temporary Mobile Subscriber Identity (TMSI) while the VLR region migrates to a new location and registers it. An attacker intercepting the radio link will be prohibited by temporarily hiding the original identity by assigning a mobile to subscribe identity (TMSI).

**(b) If only VLR and HLR have digital certificates, can a secure channel be established between the MS and VLR? ( If your answer is YES, you need to explain how.)**

Yes, a secure channel can be established between the MS and VLR even if only the VLR and HLR have digital certificates. The VLR can provide its digital certificate to the MS during the authentication process, and the MS can use this to establish a secure channel.

**Q5 – In SSL and TLS, why is there a separate Change Cipher Spec Protocol rather than including a change\_cipher\_spec message in the Handshake Protocol?**

The separate Change Cipher Spec Protocol is used in SSL and TLS because it provides a clear separation between the handshake and record protocols. This separation ensures that the record protocol is not affected by any changes made during the handshake protocol. In SSL/TLS, the Change Cipher Spec Protocol is a separate protocol that is used to signal a change in the encryption algorithm or key used for communication. This protocol consists of a single message that indicates a switch to a new encryption state. The main reason for having a separate Change Cipher Spec Protocol rather than including a change\_cipher\_spec message in the Handshake Protocol is to provide additional security.

The Handshake Protocol is used to establish the security parameters for communication, including the encryption algorithm and key. It is important that these parameters are securely established before any data is exchanged. By separating the Change Cipher Spec Protocol, the security parameters can be established separately from the actual data exchange. This ensures that the security parameters are fully negotiated and agreed upon before the data is transmitted, reducing the risk of an attacker being able to intercept and tamper with the data.

Furthermore, by separating the Change Cipher Spec Protocol, it becomes possible to change the encryption state without performing a complete renegotiation of the security parameters. This allows for more efficient use of resources, as it avoids the need to re-establish the security parameters each time the encryption state needs to be changed. Overall, the separation of the Change Cipher Spec Protocol from the Handshake Protocol provides a more secure and efficient approach to managing encryption in SSL/TLS.

**Q6 - What steps are involved in the SSL Record Protocol transmission?**

The SSL Record Protocol is responsible for fragmenting, compressing (if configured), encrypting and authenticating SSL/TLS messages before they are transmitted over the network. The steps involved in the SSL Record Protocol transmission are:

(1) fragmenting the data into manageable blocks - The message to be transmitted is divided into one or more SSL/TLS records. Each record is less than or equal to the maximum record size specified by the protocol.

(2) Compression (optional): The record data is compressed if the compression feature is enabled and negotiated between the client and server.

(3) Addition of SSL/TLS headers: Each record is assigned a header containing the type of the record, the protocol version, and the length of the record.

(4) Encryption: The record data is encrypted using the encryption algorithm and keys negotiated during the SSL/TLS handshake. The encryption provides confidentiality, which means that the data is protected from eavesdropping.

(5) Adding MAC (Message Authentication Code): The encrypted record is then processed through a Message Authentication Code (MAC) algorithm to ensure data integrity. The MAC is generated using the agreed MAC algorithm and a secret key established during the handshake.

(6) Sending: Finally, the encrypted record and MAC are sent to the destination. The recipient decrypts the record and verifies the MAC to ensure message integrity and authenticity.

This process is repeated for each SSL/TLS record that needs to be transmitted. Once all the records have been sent, the SSL/TLS session is closed.