CCM, GCM, TLS and IP-sec CCM-CCM stands for Counter with CBC-MAC (CCM) mode, which is a mode of operation for block ciphers that provides authenticated encryption. It is commonly used in information security to ensure the confidentiality, integrity, and authenticity of data. CCM mode combines the Counter (CTR) mode for encryption and the Cipher-Block Chaining Message Authentication Code (CBC-MAC) for authentication. It is suitable for resource-constrained devices like Io-T devices as it requires minimal computational resources. 1. Dividing the data: - The input data is divided into two parts: plaintext and associated data (AAD). The plaintext contains the actual message, while the AAD can include additional information that is not encrypted but is authenticated. 2. Encryption: - The plaintext is encrypted using the Counter (CTR) mode of operation, which generates a stream of cipher-text blocks. - The Counter mode uses a unique counter value for each block, combined with a nonce and a key. 3. Authentication: - The CBC-MAC algorithm is applied to the plaintext and the AAD separately. - The MAC values generated for both the plaintext and the AAD are concatenated. 4. Combining the cipher-text and MAC: - The cipher-text and the MAC value are concatenated to form the authenticated encrypted output. 5. Decryption and verification: - On the receiving end, the cipher-text is decrypted using the same Counter mode. - The CBC-MAC algorithm is applied to the decrypted plaintext and the received MAC separately. - The calculated MAC values are compared with the received MAC value. If they match, the data is considered authentic. CCM mode provides confidentiality through encryption and integrity through the CBC-MAC algorithm. It also offers authenticity as the MAC value ensures that the data has not been tampered with. This mode of operation is widely used in applications where data integrity and confidentiality are critical, such as wireless communication protocols like Wi-Fi Protected Access (WPA2) and Bluetooth Low Energy (BLE).GCM GCM (Galois/Counter Mode) is a widely used encryption mode in information security. It combines the counter mode of encryption (CTR) with the Galois mode of authentication (GMAC). GCM provides both confidentiality (encryption) and integrity (authentication) of data, making it suitable for secure communication and storage1. Key Generation: A secret key is generated using a secure key generation algorithm, typically with a suitable key size (128 bits, 192 bits, or 256 bits) depending on the desired security level. 2. Initialization: A unique initialization vector (IV) is generated for each encryption operation. The IV is typically a nonce (number used once) and should be unpredictable to ensure the security of the encryption. 3. Encryption: GCM uses the counter mode (CTR) for encryption, where a counter is encrypted and then XORed with the plaintext to produce the ciphertext. The counter value is derived from the IV and an initial counter value. This process is performed for each block of data. 4. Authentication: GCM utilizes the Galois mode of authentication (GMAC) to provide data integrity. GMAC generates a tag (also known as a MAC, message authentication code) that represents the authentication of the ciphertext. It uses a polynomial multiplication algorithm in a Galois field to compute the authentication tag5. Finalization: The encryption process is completed by appending the authentication tag to the ciphertext. To decrypt and verify the integrity of the data encrypted with GCM, the recipient uses the same secret key, IV, and the ciphertext. The recipient performs the decryption process using the counter mode (CTR) and then computes the authentication tag using GMAC. If the computed authentication tag matches the one received with the ciphertext, the data is considered authentic and has not been tampered with. TLS Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security. TLS was proposed by the Internet Engineering Task Force (IETF), an international standards organization, and the first version of the protocol was published in 1999. The most recent version is TLS 1.3, which was published in 2018What is the difference between TLS and HTTPS? HTTPS is an implementation of TLS encryption on top of the HTTP protocol, which is used by all websites as well as some other web services. Any website that uses HTTPS is therefore employing TLS encryption. Why should businesses and web applications use the TLS protocol? TLS encryption can help protect web applications from data breaches and other attacks. Today, TLS-protected HTTPS is a standard practice for websites. The Google Chrome browser gradually cracked down on non-HTTPS sites, and other browsers have followed suit. Everyday Internet users are more wary of websites that do not feature the HTTPS padlock icon. What does TLS do? There are three main components to what the TLS protocol accomplishes: Encryption, Authentication, and Integrity. Encryption: hides the data being transferred from third parties.• Authentication: ensures that the parties exchanging information• are who they claim to be. Integrity: verifies that the data has not been forged or tampered• withHow does TLS work? A TLS connection is initiated using a sequence known as the TLS handshake. When a user navigates to a website that uses TLS, the TLS handshake begins between the user's device (also known as the client device) and the web server. During the TLS handshake, the user's device and the web server: Specify which version of TLS (TLS 1.0, 1.2, 1.3, etc.) they will use Decide on which cipher suites (see below) they will use Authenticate the identity of the server using the server's TLS certificate Generate session keys for encrypting messages between them after the handshake is complete The TLS handshake establishes a cipher suite for each communication session. The cipher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for that particular session. TLS is able to set the matching session keys over an unencrypted channel thanks to a technology known as public key cryptography. The handshake also handles authentication, which usually consists of the server proving its identity to the client. This is done using public keys. Public keys are encryption keys that use one-way encryption, meaning that anyone with the public key can unscramble the data encrypted with the server's private key to ensure its authenticity, but only the original sender can encrypt data with the private key. The server's public key is part of its TLS certificate. Once data is encrypted and authenticated, it is then signed with a message authentication code (MAC). The recipient can then verify the MAC to ensure the integrity of the data. This is kind of like the tamperproof foil found on a bottle of aspirin; the consumer knows no one has tampered with their medicine because the foil is intact when they purchase it. IPsec IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it. Uses of IP Security IPsec can be used to do the following things: To encrypt application layer data.• To provide security for routers sending routing data across the• public internet. To provide authentication without encryption, like to authenticate• that the data originates from a known sender. To protect network data by setting up circuits using IPsec• tunneling in which all data being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection Components of IP Security It has the following components: Encapsulating Security Payload (ESP)• Authentication Header (AH)• Internet Key Exchange (IKE)• 1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload. 2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality. 3. Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way overSecurity Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec. Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm’s IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets that are not authorized are discarded and not given to the receiver. IP Security Architecture IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services: Confidentiality• Authenticity• Integrity•Working on IP Security The host checks if the packet should be transmitted using IPsec or• not. This packet traffic triggers the security policy for itself. This is done when the system sending the packet applies appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not. Then IKE Phase 1 starts in which the 2 hosts( using IPsec )• authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode provides greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly The channel created in the last step is then used to securely• negotiate the way the IP circuit will encrypt data across the IP circuit. Now, the IKE Phase 2 is conducted over the secure channel in• which the two hosts negotiate the type of cryptographic algorithms to use on the session and agree on secret keying material to be used with those algorithms. Then the data is exchanged across the newly created IPsec• encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs. When the communication between the hosts is completed or the• session times out then the IPsec tunnel is terminated by discarding the keys by both hosts Features of IPSec Authentication: IPSec provides authentication of IP packets using• digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged. Confidentiality: IPSec provides confidentiality by encrypting IP• packets, preventing eavesdropping on the network traffic. Integrity: IPSec provides integrity by ensuring that IP packets have• not been modified or corrupted during transmission. Key management: IPSec provides key management services,• including key exchange and key revocation, to ensure that cryptographic keys are securely managed. Tunneling: IPSec supports tunneling, allowing IP packets to be• encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol). Flexibility: IPSec can be configured to provide security for a wide• range of network topologies, including point-to-point, site-to-site, and remote access connections. Interoperability: IPSec is an open standard protocol, which means• that it is supported by a wide range of vendors and can be used in heterogeneous environments.