CSCI 530: Security Systems
Assignment 2: IPSEC; Submission Due: 15th November 2024

Name: Anne Sai Venkata Naga Saketh
USC Email: annes@usc.edu
USC ID: 3725520208

Question:

Explain how the use of IPSec to protect the confidentiality and Integrity of communications between a web browser and a web server differ from the use of SSL (or TLS). In answering this question, assume you are using only one method - even though one could employ both. In your answer, be sure to discuss how all of the keys used are negotiated (chosen and communicated), and also identify the end-points that are authenticated (is it the Web Server, the Web Browser, the User, the company running the web server, or the host running the web server).

IPsec and SSL/TLS both are required to keep our info safe, but they work in different ways. IPsec is like a guard at the entry of the network, protecting all IP traffic. SSL/TLS is like a guard at the entry of web server, making sure only the right traffic can get in and out.

IPsec

IPsec has two main modes:
1. Transport Mode: This mode encrypts only the data part of the IP packet, leaving the header unchanged. Perfect for seamless communication between a particular browser and web server.
2. Tunnel Mode: This mode encrypts the whole IP packet, including the header, and then wraps it in a new IP packet. Often used in situations where super-secret communication is needed between networks

IPsec uses two security protocols to keep things secure:
1. Authentication Header (AH): This makes sure that the data is the same as it was sent and that the intended sender only. However, in this protocol, the data is not private.
2. Encapsulating Security Payload (ESP): This keeps the data private by encrypting it using a secret code, makes sure it's the same as it was sent, and can also check if it is the intended sender.

Key Exchange process of IPsec with IKE

IPsec uses the Internet Key Exchange (IKE) protocol to set up a secure connection between two devices. IKE has two main steps:

Step 1: This step creates a safe way for the devices to talk to each other. They can use pre-shared keys, digital certificates, or public key cryptography to prove who they are. Usually, they use the Diffie-Hellman key exchange to share a secret code. In this phase, we'll be having a secret handshake to agree on encryption keys and security parameters.

Step 2: In this step, IKE makes sure that each device has the right encryption keys and other security settings for the session.

Data Encryption
At the network layer, every exchange between the browser and the server, including HTTP requests and responses are encrypted. This stops eavesdropping and guarantees confidentiality.

Endpoint Authentication in IPsec
IPsec is great for securing network-to-network or host-to-network connections. But for a web server and browser, it only checks if the device or host running the server and the client's IP are the same, not if the user or specific application is the same.

SSL/TLS
SSL is a kind of security protocol that's designed to keep your data safe when you're using the internet. It's like a secret tunnel that only you and the server can use. Unlike IPsec, which works at the network level, SSL/TLS creates a private connection between your device and the server, so no one else can see what you're doing.

Key Exchange in SSL/TLS Handshake
The SSL/TLS handshake has four main steps.
1. The client (web browser) sends its info, like the cipher suites it supports, to the server.
2. The server picks an encryption method and sends its digital certificate to the client for verification.
3. The client checks the server's certificate with a trusted authority.
4. The client uses the server's public key from the certificate to encrypt a session key and sends it to the server. Then, they both use the session keys to start communicating.

Endpoint Authentication in SSL/TLS
SSL/TLS helps you trust the website you're visiting. It uses certificates from a trusted company called a Certificate Authority to prove that the website is who it says it is.

When you use SSL/TLS, the website's secret code (session key) is only visible to you and the website. This means that only the website can decrypt the key and show you the content you want to see.

Comparison of SSL/TLS and IPsec

Factor	IPsec	SSL/TLS
Authentication Mechanism	IPsec authenticates based on IP address, which is beneficial in network-based security contexts but less effective for	SSL/TLS relies on certificates from CA, which directly verify the entity running the web server. This provides better

	application-level trust. It can authenticate devices but not specific users or applications	authentication, particularly for user-facing applications like websites
Key Negotiation	IPsec uses IKE to establish a secure connection between IP addresses. It involves a two-step process with sequence numbers to avoid replay attacks	SSL/TLS handles key exchange during the handshake process. It usually uses RSA or Diffie-Hellman for public key exchange. SSL/TLS is all about quickly setting up a secure session over HTTPS
Flexibility and Application Focus	IPsec secures all IP traffic between endpoints, making it suitable for VPNs, remote connections. Its broad protection scope is good for environments where securing entire networks or host-to-host communication is needed	SSL/TLS is optimized for securing specific applications. Its transport-layer operation ensures that application data (HTTP traffic) is encrypted while allowing other traffic to remain unencrypted if needed
Endpoint and User Protection	IPsec secures endpoints (hosts or gateways) rather than applications or users	SSL/TLS provides an application-level security model focused on user interactions

To put it briefly, SSL/TLS operates at Layer 4/5 and secures protocols like HTTP, whereas IPSec operates at Layer 3 and secures all IP packets between hosts or networks.

Benefits of Web Communications using IPSec

- **Network Layer Protection:** Regardless of the application protocol (HTTP, HTTPS, etc.), IPSec protects all traffic by operating at the network layer.
- **Transparency:** The operating system handles security; applications (such as the web browser and server) do not need to be aware of IPSec.
- **End-to-end security:** guarantees that, even while moving across insecure networks, the complete data flow is safe.