Jose Daniel Acuña Solano 2018145020

Seguridad de comunicación

IPsec

Empezó como una protección en la capa de aplicación E2E (es encriptado y desencriptado por los procesos fuente y destino), pero como esto implica que los desarrolladores entiendan e implementen seguridad esto no es siempre factible, se propone agregar protección en la capa de red (capa 3) también y así nació Ipsec según estándar RFCs 2401, 2402 y 2406. Ipsec es un conjunto de protocolos y estándares.

Firewalls

Ipsec se encarga de dejar paras lo bits “buenos” y denegar los “malos”, pero no es capaz de bloquear el acceso a LANs a posibles intrusos, este es el trabajo del *firewall*; es analógico a construir un muro alrededor de un castillo, mantiene bloqueados todos los puertos del sistema.

Los firewalls logran evitar intrusos y proteger información sensible, pero no son a prueba de todo ataque; se puede sobrecargar un sitio web enviando múltiples paquetes validos hasta saturarlo y que falle, el firewall no está diseñado para este tipo de ataques; también se pueden hacer múltiples solicitudes de conexión sin enviar respuesta para dejar al servidor en espera, estos son (DoS), donde el objetivo no es robar información, sino bloquear al objetivo.

Redes privadas virtuales

Proveen seguridad a las empresas porque aíslan la red del internet, como tener una red privada es muy costoso nacieron las VPNs, se hacen túneles entre oficinas usando Ipsec para mantener los datos encriptados. Mientras el VPN este bien configurado, este es invisible para las aplicaciones de los usuarios, pueden acceder a internet con normalidad.

Jose Daniel Acuña Solano 2018145020

Seguridad inalámbrica

Se expone las vulnerabilidades que presenta una conexión estándar 802.11, donde se puede atrapar la señal inalámbrica que va pasando por el aire e ir almacenándola en una laptop, en una conexión cableada solo se puede acceder si se tiene conectada físicamente, por lo que las redes inalámbricas son mas sensibles a ataques.

Bluetooth tiene menor rango, pero igual corre el riesgo que 802.11, este protocolo tiene sistemas de seguridad en múltiples capas, por ejemplo: ingresar un código PIN en capa de aplicación; encriptar los datos totalmente; claves simétricas tradicionales.

WAP 2.0 usa estándares conocidos en todas las capas, por lo que de manera promediada es más seguro que 802.11 y Bluetooth en, privacidad, autenticación e integridad.