Resumen #8 - (r8)

Esteban Ignacio Durán Vargas - 2020388144

IC - 7602 - 2023 I Semestre

8.6 SEGURIDAD EN LA COMUNICACIÓN

8.6.1 IPsec

La encripción de ambos extremos tenía problemas. Requería cambiar a todas las aplicaciones para que estuvieran conscientes de esta; sino ponerlo en una nueva capa antes de aplicación. El otro es que los usuarios no entienden esta seguridad; entonces los usuarios no deben autenticar sino la red. Salió IPsec que requería cifrado todo el tiempo pero permitía el uso de un algoritmo nulo, rápido y simple. IPsec son servicios, algoritmos y granularidades. Los servicios es que no todos quieren pagar siempre, algunos son confidencialidad, integridad de datos y protección contra ataques de repetición. Estos se basan en criptografía simétrica. Hay múltiples algoritmos porque pueden dejar de ser seguros y es mejor que sean independientes. Multiples granularidades porque que haya protección de una sola conexión TCP, todo el tráfico entre un par de hosts o enrutadores seguros, y otros.

Se encuentra en la capa IP, es orientado a conexión. Se requiere una clave por un periodo. Se amortizan costos de configuración sobre muchos paquetes. Una conexión es un SA (asociación de seguridad), conexión simplex entre dos puntos y tiene un identificador de seguridad. Si requiere en ambas direcciones se ocupan dos SA. Los identificadores viajan en las conexiones para buscar claves y otra información del paquete.

IPsec tiene 2 partes: dos encabezados nuevos para el paquete para transportar el identificador, datos de control de integridad, etc; y ISAKMP (Asociación para seguridad en Internet y Protocolo de Administración de Claves), que establece las claves y su protocolo principal IKE (intercambio de claves de internet) está plagado de fallas. IPsec puede utilizarse en cualquier modo: transporte donde el encabezado se inserta justo después del encabezado IP, el campo Protocolo se cambia para indicar que el encabezado IPsec sigue al normal que contiene la información de seguridad (SA, número de secuencia, verificación de integridad...); y el modo tunel donde todo el paquete se encapusula dentro de uno nuevo, donde por lo general el paquete no termina en el destino final y el final del túnel es una máquina de puerta de enlace de seguridad como un firewall que encapusla y desencapsula paquetes confrome pasan y así las máquinas no saben de IPsec. El túnel también sirve cuando se agregan conexiones TCP y se maneja un solo flujo cifrado porque así se evita que un intruso vea a quién se envían los paquetes. El estudio de patrones de flujo es análisis de tráfico y túnel lo frustra pero agrega un encabezado extra y aumenta el tamaño de paquete. El primer nuevo encabezado es AH (autenticación) que propociona verificación y seguridad antirrepetición pero no la confidencialidad. En el IPv4 se coloca entre el IP y TCP, y en IPv6 es solo otro de extensión. El campo Siguiente encabezado almacena el valor anterior de Protoclo IP, Longitud de carga útil es una palabra de 32 bits en el encabezzado AH menos 2, el Índice de parámetros de seguridad es el indicador de registro en paricular en la base de datos receptor y contiene la clave compartida de la conexión y otra información sobre esta, el campo de Número de secuencia numera todos los paquetes y obtiene un número único para evitar ataques de repetición; y finalmente el campo de Datos de autenticación contiene la firma digital. Cuando se establece la SA ambos lados negocian el algoritmo firma y no se utiliza la criptografía de clave pública porque los paquetes se procesan muy rápido y esos son lentos. IPsec se basa en clave simétrica y el emisor y receptor negocian la clave antes de establcer el SA. Una forma es calcular el hash sobre el paquete más clave compartida. HMAC (Código de autenticación

de mesnajes basado en HASH) es un esquema de estos. El encabezado AH no permite encriptación de datos, útil cuando la integridad de datos (abarca campos en el encabezado IP, principalmente los que no cambian cuando el paquete se mueve de enrutador) es necesaria pero la confidencialidad no. El campo de tiempo de vida cambia en cada salto entonces no se incluye en la verificación de integridad pero la IP de origen si entonces no se puede falsificar.

El encabezado IPsec alternativo es ESP (Carga útil de encapsulamiento de seguridad) consiste en 2 palabras de 32 bits y son los campos índice de parámetros de seguridad y número de secuencia; además a veces una tercera es el vector de inicialización para encriptar datos. ESP incluye verificaciones HMAC pero se inclueyn en la carga útil y se tiene la ventaja de implementación de hardware y se puede calcular conforme los bits se transmiten por la interfaz de red y agregarse al final. Con AH se almacena en el búfer y la firma se calcula antes de enviar el paquete pero es más lento.

AH antes solo era integridad, ESP confidencialidad, pero se le agregó integridad y no se quería dejar morir AH y decían que era porque verifica parte del encabezado IP y ESP no lo hace.

8.6.2 Firewalls

Servidores de seguridad. Se obliga a todo el tráfico a pasar por un firewall. Tiene dos componentes: 2 enrutadores que filtran paquetes y una puerta de enlace de aplicación. Cada filtro es un enrutador equipado con una funcionalidad extra e inspecciona cada paquete entrante o saliente. Si cumplen un criterio se reenvían. El objetivo de la dos filtros diferentes en 2 LANs diferentes es asegurar que ningún paquete pase sin pasar por la puerta de enlace de aplicación. Los filtros son manejados por tablas configuradas por administrador del sistema, que listan origenes/destinos aceptables/bloqueado y las reglas permitidas. Los origenes y destinos son IP y un puerto para TCP/IP. Bloquear paquetes salientes es difícil porque no todos los sitios siguen las numeraciones de puertos. Algunos (FTP) los asignan aleatorio. UDP es difícil saber qué harán y hay paquetes que los prohiben del todo. La puerta de aplicación opera a nivel de aplicación y puede descartar, ejemplo, correos según su contenido, tamaño, etc. Pueden tener más puertas de enlace para aplicaciones específicas.

Puede haber problemas, como que se introduzcan direcciones de origen falsas para evadir verificación, encriptar contenido para que pase por filrtos y que el 70% de ataques pasan del lado interno. También se puede enviar paquetes legítimos al destino hasta que el sitio se caiga (DoS), los paquetes tienen direcciones falsas de orígenes y no pueden ser rastreados. A veces son cientos de computadoras y lo hace difícil de detectar y ese es DDOS (negación de servicio distribuida).

8.6.3 Redes privadas virtuales

Una red privada es constituida por computadoras de compañías y líneas telefónicas alquiladas. Son seguras, el tráfico no se fuga y solo se puede intervenir físicamente; pero es costoso. Hubo demanda de trasladar tráfico de datos a red pública sin renunciar a seguridad y aparecieron las redes privadas virtuales que están superpuestas sobre redes públicas pero tienen características de privadas. Es popular construirlas en internet. Cada oficina tiene un firewall y crea túneles entre cada oficina. Si se usara IPsec entre las oficinas se podría usar una SA encriptada y autenticada para proporcionar control de integridad, confidencialidad e innmunidad a análisis de tráfico. Cada firewall negocia parámetros de se SA con servicios, modos de algoritmos y claves. Algunos tienen capacidad VPN integrada. Con los SAs el tráfico fluye; el paquete viaja a través de un túnel VPN con un encabezado IPsec después del IP pero como no tienen efecto en el proceso de reenvío los enrutadores no se preocupan. De esta manera, los VPN son transparentes para todo el software de usuario.

Los firewalls configuran y manejan las SAs y la única persona que sabe de esto es el administrador del sistema quien configura y maneja los firewalls.

8.6.4 Seguridad inalámbrica

Por lo general los endpoints se saltan seguridad y empiezan a operar y cualquiera puede interceptarlos.

- **Seguridad del 802.11**

  WEP (Privacidad Inalámbrica Equivalente) es un protocolo en nivel de la capa de de enlace de datos. Lo hace tan seguro como una LAN. Cada estación tiene una clave que comparte con la base, solo pueden ser precargadas por el fabricante y se intercambian a través de la red. La base pueden tomar una clave y enviarla a otro con la clave pública del otro. El cifrado de flujo es con algoritmo RC4 y fue secreto hasta que fue filtrado en 1994. Genera un flujo que aplica un OR exclusivo con un texto llano.

  Para encriptar se realiza un cheksum de la carga útil con CRC-32 polinomial y se agrega a la carga útil para formar parte del texto llano para el algoritmo de encriptación; se le aplica un XOR con un fragmento de flujo de claves y el resultado es el texto cifrado. El IV que inicia el RC4 se envía con el texto y cuando se recibe se extrae la carga, genera el flujo de claves a partir de la clave secreta compartida y el IV que recibió y aplica un XOC al este para recuperar el texto y comprobar el checksum. Hay métodos para violarla; muchas instalaciones usan la misma clave compartida y cada usuario puede leer todo el tráfico de los demás. Aún si no,las claves son estables por mucho tiempo y se recomienda cambiar cada paquete para evitar reutilización de flujos de claves; las portatiles restablecen el IV a 0 cuando se introduce la tarjeta en la computadora, esto hace común número bajos de IV y puede permitir recalcular el XOR. Además estos son solo de 24 bits, por lo que solo ocupa 5000 paquetes para que use el mismo IV. Como los IVs son aleatorios, se puede crear un par valido para generar todos los paquetes que desee que lo utilicen e interferir en la comunicación. El CRC no es de ayuda porque se calcula con la carga útil entonces es solo cambiarlo.

  Se encontró en 2001 que muchas de las claves tienen la propiedad de derivar algunos bitrs de las claves con el flujo. La IEEE respondió que: WEP no era mejor que Ethernet, es peor olvidarse establecer seguridad, que usen otra seguridad, que la 802.11i será mejor, que certificaciones futuras la requerirán y que hay que ver qué se hace con esta.

- **Seguridad de Bluetooth.**

  Con menos rango pero se puede interceptar. Tiene un complejo esquema de seguridad. Si se deshabilita, no hay. Tiene 3 modos: ninguno, encriptación completa, control de integridad. En la capa física los saltos proporcionan poco de seguridad, pero hay que indicarle a cuál secuencia de saltos de frecuencia de una piconet es el dispositvo, lo que no lo hace secreto. Cuando le pide un canal al maestro se supone que ambos comparten clave. En otros casos un dispositvio la tiene integrada y el usuario tiene que introducir esa clave en otro dispositivo (claves maestras). Para establecer un canal se verifica si otro conoce la clave maestra, negocian el canal, encripción y/o integridad. Después seleccionan una clave de sesión aleatoria de 128 bits donde algunos son públicos para que se puedan romper por el gobierno.

  La encriptación es E0, control de integridad es SAFER+. Ambos utilizan clave simétrica. SAFER+ se escogió para Bluetooth a pesar de ser lento porque aún no se escogía AES.

Al texto llano se le aplica XOR con el flujo de claves para generar el texto cifrado. E0 es similar a A5/1 que tuvo una falla grande. Otro problema de Bluetooth solo autentica dispositivos no usuarios. Bluetooth también implementa seguridad en capas superiores; aún con una brecha en capa de enlace, hay algo de seguridad.

- **Seguridad de WAP 2.0**

  Utiliza protocolos estándar en todas las capas. Soporta IPsec, en capa de red. En capa de transporte las conexiones TCP puede protegerse con TLS, estándar IETF. Usa autenticación de cliente HTTP. Las crypto bibliotecas a nivel de aplicaciones dan control de integridad y de no repudio. Puede tener mejores seguridad que 802.11 y Bluetooth.