Jonder Hernández Gutiérrez

IPSec

La **IETF (Internet Engineering Task Force)** ha sabido por años que existe una gran necesidad por seguridad en Internet. La mayoría de los expertos en seguridad creían que para ofrecer una verdadera seguridad, el sistema de cifrado y las verificaciones de integridad tenían que llevarse a cabo de extremo a extremo. El problema con este enfoque es que requiere cambiar todas las aplicaciones para que estén conscientes de la seguridad. Desde esta perspectiva, el siguiente enfoque más conveniente es colocar el encriptado en la capa de transporte o en una nueva capa entre la capa de aplicación y la de transporte, con lo que se conserva el enfoque de extremo a extremo, pero no hay que cambiar las aplicaciones.

La perspectiva opuesta es que los usuarios no entiendan la seguridad y no sean capaces de utilizarla de manera correcta, así como que nadie desee modificar los programas existentes de ninguna forma, por lo que la capa de red debe autentificar o encriptar paquetes sin que los usuarios estén involucrados. Después de años de batallas encarnizadas, esta perspectiva ganó suficiente soporte como para definir un estándar de seguridad de capa de red.

El resultado de esta guerra fue un diseño llamado **IPsec (Seguridad IP, del inglés IP security)**. No todos los usuarios desean encriptado, por esta razón, en lugar de hacerlo opcional, se decidió requerir siempre pero permitir el uso de un **algoritmo nulo**. Este algoritmo nulo se describe y alaba por su simplicidad, facilidad de implementación y gran velocidad en el **RFC 2410**.

El diseño IPsec completo es un marco de trabajo para múltiples servicios, algoritmos y niveles de granularidad. La razón de los servicios múltiples es que no todas las personas quieren pagar el precio por tener todos los servicios todo el tiempo, por lo que están disponibles en todo momento.

Técnicamente, IPsec tiene dos partes principales. La primera describe dos encabezados nuevos que se pueden agregar a los paquetes para transportar el identificador de seguridad, los datos de control de integridad y demás información. La otra parte, **ISAKMP (Asociación para Seguridad en Internet y Protocolo de Administración de Claves)**, se encarga de establecer las claves.

IPSec se puede usar de dos diferentes modos, uno de ellos es el modo de transporte en el cual el encabezado IPSec se inserta justo después del encabezado del IP. Por otra parte, en el modo túnel todo el paquete IP se encapsula en el cuerpo de una IP nuevo con el encabezado totalmente nuevo.

Firewalls

Para los usuarios domésticos navegar por internet es mucha diversión, pero para los gerentes empresariales es una pesadilla de seguridad, donde es posible filtración de estrategias de marketing, planes de desarrollo de productos, secretos comerciales, etc.

Además del peligro de la fuga de información, también existe el peligro de la infiltración de información. En particular, los virus, gusanos y otras pestes digitales pueden abrir brechas de seguridad, destruir datos valiosos y hacer que los administradores pierdan mucho tiempo tratando de arreglar el daño que hayan hecho.

En consecuencia, se necesitan mecanismos para mantener los bits “buenos” dentro y los bits “malos” fuera. Un método es utilizar IPsec

Sin embargo, IPsec no hace nada por proteger a la LAN de la compañía contra las pestes digitales y los intrusos. Para saber cómo alcanzar ese objetivo, necesitamos dar un vistazo a los firewalls.

Los **Firewalls** son simplemente una adaptación moderna de la vieja estrategia medieval de seguridad de excavar un foso defensivo profundo alrededor de su castillo. Este diseño obligaba a que todos los que entraran o salieran del castillo pasaran a través de un único puente levadizo, en donde los encargados de la E/S los pudieran inspeccionar. En las redes es posible el mismo truco.

El firewall actúa como un filtro de paquetes. Inspecciona todos y cada uno de los paquetes entrantes y salientes. Los paquetes que cumplen cierto criterio descrito en reglas formuladas por el administrador de la red se reenvían en forma normal. Los que fallan la prueba simplemente se descartan. Por lo general, los criterios de filtrado se proporcionan como reglas o tablas que listan los orígenes y destinos aceptables, los orígenes y destinos bloqueados y las reglas predeterminadas acerca de lo que se debe hacer con los paquetes que entran y salen a otras máquinas.

Existe una clase de ataques que los firewalls no pueden manejar. La idea básica de un firewall es evitar que entren intrusos y que salga información secreta. Por desgracia, hay personas que no tienen nada mejor que hacer que tratar de inhabilitar ciertos sitios. Para ello envían grandes cantidades de paquetes legítimos al destino, hasta que el sitio se colapsa debido a la carga.

Seguridad Inalámbrica

Es muy fácil diseñar un sistema mediante el uso de redes VPN y firewall que sea completamente seguro, pero eso, en la práctica, puede fallar. Esta situación puede ocurrir si algunas de las máquinas son inalámbricas y utilizan comunicación de radio, la cual pasa justo encima del firewall en ambas direcciones.

El rango de las redes 802.11 es muy amplio y puede llegar a cientos de metros, por lo que cualquiera que lo quiera puede espiar una comunicación donde podrían hacer un ataque **MITM (Hombre en el medio del inglés Man In The Middle)**, este consiste en escuchar una comunicación y hacer que las dos partes crean que se están comunicando entre sí mientras se inserta en medio de la comunicación sin ser detectado. Esto puede ir de escuchar conversaciones por correo o hasta enviar correos falsos pretendiendo ser otra persona. En teoría, se supone que esta fuga no debería suceder. Pero, en teoría, las personas tampoco deberían robar bancos.

Seguridad del 802.11

Una parte del estándar 802.11 establece un protocolo de seguridad en el nivel de enlace de datos para evitar que un nodo inalámbrico lea o interfiera con los mensajes enviados entre otro par de nodos inalámbricos. También se le conoce mediante el nombre comercial **WPA2 2 (Acceso Protegido WiFi 2)**. Este es un reemplazo para el esquema **WEP (Privacidad Equivalente a cableado)**, el WEP fue diseñado por un comité de estándares de redes.

Al analizar el esquema WEP se encontraron resultados devastadores. ¿Qué era lo que estaba mal? Pues resulta que casi todo, desde la perspectiva de seguridad. Por ejemplo, para encriptar los datos confidenciales, el WEP

les aplicaba un OR exclusivo con la salida de un sistema de cifrado de flujo. Por desgracia, los arreglos de claves débiles significaban que la salida se reutilizaba con frecuencia.

Hay dos escenarios comunes en los que se utiliza el esquema WPA2. El primero es en un entorno corporativo, en donde una empresa tiene un servidor de autentificación separado con una base de datos de nombres de usuario y contraseñas, la cual se puede usar para determinar si un cliente inalámbrico puede o no acceder a la Red. En este entorno, los clientes usan protocolos estándar para autentificarse con la Red

Seguridad de Bluetooth

Bluetooth tiene un rango mucho más corto que el 802.11, por lo que no es fácil atacarlo desde un estacionamiento, pero la seguridad sigue siendo un problema en este caso. Por ejemplo, podrían utilizar un ataque de **MITM (Man In The Middle)** mencionado anteriormente para escuchar una conversación entre dos personas.

La seguridad en Bluetooth se proporciona en varias capas. En la capa física los saltos de frecuencia proporcionan un poco de seguridad, pero debido a que se necesita indicar a cualquier dispositivo Bluetooth de una piconet la secuencia de saltos de frecuencia es correcto decir que esta secuencia no es secreta.

Cada dispositivo, por ejemplo un auricular, tiene una clave integrada fija y el usuario tiene que introducirla en el otro dispositivo. Estas claves se conocen como **claves de acceso**, por desgracia estas claves comúnmente se establecen en "1234" o cualquier otro valor predecible. Para establecer un canal, tanto el esclavo como el maestro verifican si el otro conoce la clave de acceso. De ser así, negocian si ese canal será encriptado, si se controlará su integridad o ambas cosas.