Resumen

8.6.1: IPSec

Hay falta de seguridad en internet, agregarla no era fácil, se encontró una forma de añadirla pero había un problema que implicaba cambiar todas las aplicaciones para que supieran esa seguridad por lo que se pensó en colocar el cifrado 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 requiere que se cambien las aplicaciones. Al final se argumentó que tener cifrado de la capa de red no evitaba que los usuarios conscientes de la seguridad la aplicaran correctamente y que ayudaba hasta cierto punto a los usuarios no conscientes de ella.

El resultado fue un diseño llamado IPsec (Seguridad IP), que se describe en los RFCs 2401, 2402 y 2406, entre otros. No todos los usuarios desean cifrado (pues éste es costoso computacionalmente). En lugar de hacerlo opcional, se decidió requerir cifrado todo el tiempo pero permitir el uso de un algoritmo nulo. IPsec completo es una estructura para servicios, algoritmos y granularidades múltiples la razón es que no todas las personas ocupan todos los servicios. Los servicios principales son confidencialidad, integridad de datos y protección contra ataques de repetición (un intruso repite una conversación).

Todos son basados en criptografía simétrica. La razón de tener múltiples algoritmos es por si lo rompen en un futuro el ipsec puede sobrevir ya que la estructura es independiente y la razón de tener múltiple granularidad es hacer segura la conexión entre 2 host. Ipse es orientado a la conexión, una conexión en ipsec es conocia como SA(conexión simplex entre 2 puntos con un identificador de seguridad). Para tráfico seguro entre 2 conexiones se necesita 2 asociaciones.

IPsec tiene 2 partes: 2 encabezados y ISAKMP. Ipsec puede usarse en el modeo de Transporte (encabezado ipsec se inserta justo despues de encabezado IP), modo Túnel(todo se encapsula dentro del cuerpo del IP, útil cuando se agrega un conjunto de conexiones TCP y se maneja como un solo flujo cifrado, base militar, casa blanca). El problema de túnel es que se aumenta el tamaño del paquete porque se agrega la ip.

Análisis de tráfico: estudio de patrones de flujo de paquetes. El encabezado AH proporciona verificación de integridad y seguridad antirrepetición, pero no la confidencialidad.IPsec se basa en la criptografía simétrica.

Si ESP hace lo que hace AH y más por qué no solo usar ESP? La respuesta es histórica, no se quería dejar morir por lo que se argumentó que que AH verifica parte del encabezado IP a diferencia de ESP. Otra es que un producto con AH no tiene problemas con licencias de exportacion ya que no puede encriptar.

8.6.2: Firewalls

Conectar una computadora en cualquier lugar tiene muchas ventajas, pero las personas que necesitan mantener información confidencial no les sirve. Ademas de filtración de datos también hay infiltración por medio de virus. Una solución para este problema es usar ipsec pero solo sirve cuando se transporta la información y no sirve para mantener afuera las pestes.

Firewall(servidores de segurridad): cavar un foso profundo alrededor del castillo por lo que todos los que quisieran entrar o salir tienen que pasar por el puente en donde podían ser inspeccionados. Lo mismo pasa con las compañias, todos pueden entrar y salir del tráfico de red pero pasando por el puente.

Firewall tiene dos componentes: dos enrutadores que realizan filtrado de paquetes y una puerta de enlace de aplicación con la ventaja de pasar por dos filtros y una puerta de enlace. Un firewall que consiste en dos filtros de paquetes y en una puerta de enlace de aplicación. Los paquetes que cumplan con los criterios pasan sino se descartan.

Los paquetes que cruzan la primera barrera pasan a la puerta de enlace donde se vuelven a examinar. El objetivo de colocar los dos filtros de paquetes en LANs diferentes es asegurar que ningún paquete entre o salga sin pasar a través de la puerta de enlace de aplicación: no hay otra ruta. Los filtros son manejdaos por tablas configuradas por el admin. Bloquear paquetes salientes es difícil, tcp es dificil pero UDP aún más ya que no se sabe loq ue hará.

La segunda mitad del firewall es la puerta de enlace de aplicación: opera a nivel de aplicación, es posible configurar puerta de en enlace para examinar cada mensaje y ver si se permite o no, porque en una instalación militar un mensaje con la palabra bomba o nuclear es muy delicada.

AUnque firewall esté configurado bien, por ejemplo si solo se permite paquetes de una red, un intruso puede introducir direcciones falsas para evadir la verificación. Dato es que 70% de los ataques de firewall vienen desde a dentro. También se puede botar un sitio web enviando montones de paquetes legítimos, esto se hace llenando la tabla y que no pueda atender a nadie más.

- Dos: cuando se s bloquea el destino en lugar de robar datos, los paquetes de solicitud tienen direcciones falsas de origen por lo que el intruso no puede ser rastreado con facilidad.
- DDoS (negación de servicio distribuida): intruso ha entrado en cientos de computadoras en cualquier parte del mundo, y después ordena a todas ellas que ataquen al mismo objetivo.

8.6.4: Seguridad en redes inalámbricas

Diseñar un sistema que sea lógica y completamente seguro mediante VPNs y firewalls es muy fácil pero falla si algunas máquinas son inalámbricas. Rango de redes 802.11 con frecuencia es de algunos cientos de metros por lo que se puede espiar a la empresa desde el parqueo de la compañia. La seguridad es mas importante en la parte inalambrica que la cableada.

Seguridad del 802.11

Establece un protocolo de seguridad a nivel de capa a enlace a datos llamado WEP, diseñado para que la seguridad de una lan inalambrica sea tan buena como la cableada. CUando se establece seguridad para estandar 802.11 cada estacion tiene clave secreta que comparte con estacion base, pueden intercambiarse por wireless, las claves duran meses o años.

WEP encripta basandose en RC4, se implmentó una estrategia para encriptar basada en suma de verificación pero fue violada, incluso si cada usuario tiene una clave distinta, WEP aún puede ser atacado. WEP recomienda (no obliga) que el IV se cambie en cada paquete para evitar los ataques de reutilización de flujo de claves pero no funciona por la tarjeta.

Es muy sencillo violar la seguridad del 802.11. IEEE respondió al hecho de que WEP se había roto por completo emitiendo una corta declaración en la que señalaba seis puntos:

1. Les dijimos que la seguridad de WEP no era mejor que la de Ethernet.
2. Es mucho peor olvidarse de establecer alguna clase de seguridad.
3. Traten de utilizar otro tipo de seguridad (por ejemplo, seguridad en la capa de transporte).
4. La siguiente versión, 802.11i, tendrá mejor seguridad.
5. La certificación futura requerirá el uso del 802.11i.
6. Trataremos de determinar qué hacer en tanto llega el 802.11i.

Seguridad de Bluetooth

Si tengo un teclado Bluetooth y no tuviese seguridad, puedo interceptarlo y saber todo lo que escribe la persona, lo mismo pasa con una impresora por tal razón posee una buena seguridad.

Bluetooth proporciona seguridad en múltiples capas: En la capa física, los saltos de frecuencia. Claves maestras: por ejemplo auriculares en donde tengo que anotar el numero de conexión en el celular. Para establecer un canal, tanto el esclavo como el maestro verifican si el otro conoce la clave maestra. De ser así, negocian si ese canal será encriptado. La encriptación utiliza un cifrado de flujo llamado E0; el control de integridad utiliza SAFER+ pero fue elimando.

Bluetooth sólo autentica dispositivos, no usuarios, por lo que el robo de un dispositivo Bluetooth podría conceder acceso al ladrón a la cuenta financiera del usuario. Pero para esto hay solución usando PIN.

Seguridad de WAP 2.0

En su mayor parte, WAP 2.0 utiliza protocolos estándares en todas las capas. Está basado en el IP, soporta el uso completo de IPsec en la capa de red. conexiones TCP pueden protegerse mediante TLS, un estándar IETF. Crypto bibliotecas a nivel de aplicación proporcionan control de integridad y de no repudio. WAP 2.0, hay una posibilidad de que sus servicios de seguridad. Privacidad, autenticación, control de integridad y no repudio pueden que sean mejores que la seguridad del 802.11 y Bluetooth.