Universidad Nacional Autónoma de México
Facultad de Ciencias
Criptografía y Seguridad

Reporte de temas a presentar en exposición
Protocolos de seguridad: IPSec, Secure Shell, TLS y PGP

Ángel Iván Gladín García
No. cuenta: 313112470
angelgladin@ciencias.unam.mx

21 de Mayo 2019

1. IPSec (p. 615 - 622)

Puntos clave:

- *IPSec* tiene la capacidad de que puede ser agregado tanto a versión actual del protocólo de internet (IPv4 o IPv6) mediante cabeceras adicionales.
- *IPSec* abarca tres áreas funcionales: autenticación, confidencialidad y manejo de llaves.
- La autenticación puede ser aplicada al paquete completo original IP (modo tunel) o a todo el paquete a excepción de la cabecera IP.
- Se proporciona confidencialidad por un fromato de cifrado conocido como encapsulamiento de seguridad del *payload*. Tanto el tunel y los modos de transporte pueden ser adaptados.

Implementado seguridad al nivel de IP, una organización puede asegurar interconexión segura, no solo para las aplicaciones que tienen mecanismos de seguridad también para muchas aplicaciones que no siguen medidas de seguridad.

Los niveles de seguridad engloban tres áreas operativas:

- **Autenticación**: El mecanismo de autenticación asegura que un paquete recibido era de hecho transmitido por uns grupo identificado como la fuente de la cabecera del paquete. Además éste mecanismo asegura que que el paquete no ha sido alterado en el camino.
- **Confidencialidad**: La habilidad de la confidencialidad permite que los nodos que se están comunicando cifren sus mensajes para prevenir su espionaje por aplicaciones de terceros.
- **Manejo de llaves**: La característica del manejo de llaves se *preocupa* que el intercambio de llaves sea seguro.

Aplicaciones de IPSec: IPSec provee la capacidad de tener una comunicación segura a través de LAN, a través de WANs privadas y públicas, y también a través del internet.

- Una conexión segura a internet en surcursales o negocios que dependen mucho en internet y reduce su necesidad de hacer una red privada, ahorrándose constos en el manteniento de una red interna.

- Un acceso remoto seguro sobre el intenet.
- Estableciendo una comunicación *extranet* e *intranet* con una asociación o campañia, esto eque IPSec puede ser usado para tener una conexión segura con otra organización, asegurando así la autenticación y confidencialidad y proviendo un mecaninso de intercambio de llaves.
- Mejorando la seguridad del comercio electrónico, aunque esos portales web ya tengan tengan incluidas herramientas de seguridad, IPSec mejora la seguridad. Garantizando que todo el tráfico sea tanto cifrado y autenticado, agregando una capa adicional de seguridad.

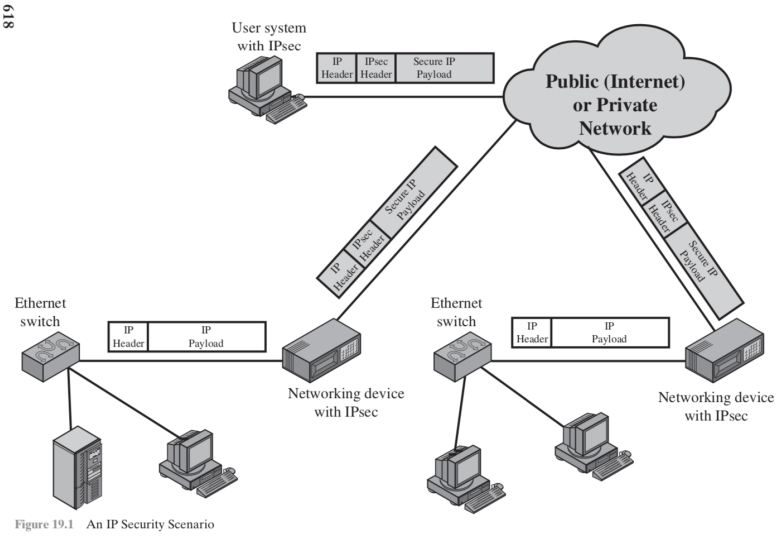

Figura 1: Un escenario típico del uso de IPSec.

Beneficios de IPSec:

- Cuando IPSec es implementado en un *firewall* o en un *router*, provee una fuerte seguridad que puede ser aplicado a todo el tráfico.
- El *firewall* en IPSec resistente a un *bybass* por tráfico de afuera.
- IPSec está por debajo de de la capa de transporte (TCP, UDP) lo que significa que es "invisible" para las aplicaciones. No hay necesidad de cambiar el *software*.
- IPSec puede ser transparente para los usuarios finales. No hay necesidad de entrenar a los usuarios en mecanismos de seguridad.
- Si se necesita, IPSec puede proveer seguridad individual a los usuarios. Esto es útil para crearles una subred privada virtual entre la organización para aplicaciones con contendido sensible.

Documentos IPSec: La totalidad de la especificaciones IPSec están dispersas entre docenas de RFCs y borradores de documentos IETF. La mejor forma comprender el alcance de IPSec es consultando la última versión del de IPSec. El documento puede ser categorizado en los siguientes grupos.

- Arquitectura
- Cabecera de autenticación (AH)
- Encapsulando la seguridad de *payload* (ESP)
- Intercambio de llaves de internet (IKE)
- Algoritmos criptográficos
- Otros

Servicios de IPSec: IPSec provee de servicios de seguridad en la capa de IP permitiendo a un sistema seleccionar los protocolos de seguridad requeridos, determinar el algoritmo a ser usado para el servicio y poner en su lugar cualquier llave criptográfica requerida para proveer los servicios solicitados.

- Control de accesos
- Integridad sin conexión
- Autenticación de información de origen
- Confidencialidad (cifrado)
- Confidencialidad de flujo de tráfico limitado

2. Secure Shell (SSH) (p. 508 - 518)

Secure Shell (SSH) es un protocolo para la comunicación segura de redes diseñado para ser relativamente simple y que su implementación no sea costosa. La versión incial SSH1 fue enfocada en proveer un mecanismo de remoto seguro de incio de sesión para remplazar a TELNET y otros clientes remotos de incio de sesión que proveían seguridad per se. Una nueva versión, SSH2 arregló muchas fallas de seguridad del esquema original. Las aplicaciones de cliente y servidor SSH están extensamente disponibles en la gran mayoría de los sistemas operativos. Ha sido el método de elección para incio de sesión remoto.

SSH está roganizado como tres protocolos que tipicamente se ejecutan encima de TCP.

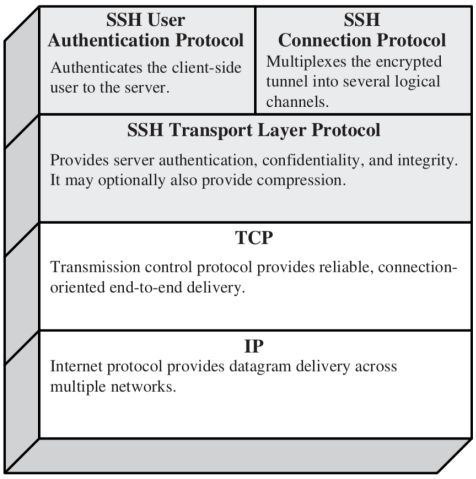

Figura 2: Pila de protocolo SSH

- **Protocolo de capa de transporte**: Provee autenticación por parte del servidor, confidencialidad e integridad de la información conconfidencialidad directa.
- **Protocolo de autenticación de usuario**: Autentica al usuario con el servidor.
- **Protocolo de conexión**: Multiplexa múltiples comunicaciones de canales lógicas sobre una sola conección SSH subyacente.

3. Transport Layer Security (TLS) (p. 502 - 506)

TLS es una inciativa de estandarización de IETF cuya meta es produir una versión de internet estándar de SSL. TLS es definidos como una propuesta estándar de internet en el RFC 5246. RFC 5246 es muy similar a SSLv3.

Número de versión: El formato de registro del TLS es el mismo al del SSL

Código de mensaje de autenticación: Hay dos diferencias entre los esquemas SSLv3 y el TLS MAC: el algoritmo actual y el alcance del calculo del MAC. TLS hace uso del algoritmo HMAC definido en RFC2014.

Funciones pseudoaleatorias: TLS hace uso de funciones pseudoaleatorias concida como PRF para expandir secretos en bloques de información para fines de generación de llave o validación. El objetico es haaer uso de un valor secreto relativamente pequeño pero para generar bloques más grandes de información de forma que sea segura de todo tipo de ataque hecho en una función hasj y MACs.

Código de alerta: TLS soporta todos los código de alerta definidos en SSLv3 con la excepción de `no_certificate`.

Juego de cifrados: Hay varias pequeñas diferencias entre los juegos de cifrados disponibles sobre SSLv3 y sobre TLS:

- **Intercambio de llave**: TLS soporta todas las técnicas de intercambios de llave de SSLv3 con la excepción de Fortezza.
- **Algoritmos de cifrado simétrico:** TLS incluye todos los algoritmos de cifrado simétrico encontrados en SSLv3, con la excepción de Fortezza.

4. Pretty Good Privacy (PGP) (p. 568 - 587)

PGP es un fenómeno notable. En gran parte por el esfuerza de una sola persona, Phil Zimmermann. PGP provee un servicio de confidencialidad y autenticación que puede ser usado para correo electrónico y aplicaciones de almacenamiento de archivos. En esenci, Zimmermann hizo lo siguiente:

- Seleccionó los mejores algoritmos criptográficos disponibles como bloques de construcción.
- Integró esos algoritmos en una aplicación de propósito general que es independiente del sistema operativo y el procesadro, y está basado en un pequeño conjunto de comandos sencillos de usar.
- Hace el paquete y su documentación, incluyendo el código fuente, libremente disponible en internet.

- Entró a un acuerdo con una compañía para proveer compatibilidad completa, un versión comercial de bajo costo PGP.

PGP ha crecido exponencialmente y ahora es extensamente usada. Un número de sus razones pueden ser citadas por su crecimiento.

- Está disponible libre al rededor del mundo en versiones que pueden ser ejecutadas en nariedad de plataformas incluyendo Windows, UNIX, Macintosh y muchas otras más. En adición a ello, la versión comercial satisface a los usuarios que quieren un producto que venga con soporte del vendedor.
- Está basado en algoritmos que han sobrevivido a la reseña del público general y son considerados extremadamente seguros. Específicamente, el paquete que incluye RSA, DSS, y Diffie-Hellman para cifrado de llave pública.
- Tiene un amplio rango aplicabilidad para corporaciones que desean seleccionar y mejorar un esquema de estandarización para cifrado de archivos y mensajes a individuos que deseen comunicarse seguramente con otros en todo el mundo sobre el internet y otras redes.
- No es controlado por ningun gobierno o una organización que da ese estándar.
- PGP es ahora un estandar de internet.

Referencias

[1] Stallings, William, *Cryptography and Network Security: Principles and Practice*, 5a Ed., Pretince Hall, 2010.