IPSec

Christofer Fabián Chávez Carazas
Universidad Nacional de San Agustín de Arequipa
Escuela Profesional de Ciencia de la Computación
Computación Centrada en Redes

24 de septiembre de 2017

IPsec (*Internet Protocol security*) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado. Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

El IP sec responde a tres principios:

- **Confidencialidad:** Los paquetes no pueden ser visto mientras transitan por el medio. Esto se logra cifrando los datos.
- **Integridad:** Los paquetes no pueden ser modificados. Se calcula el *checksum* o el valor hash de los datos.
- **Autenticación:** Asegurarse de la identidad del emisor. Se logra con firmas y certificados.
- **No Repudiación:** Garantizar que el remitente de un mensaje no pueda negar haber enviado el mensaje y que el destinatario no pueda negar que recibió el mensaje. Se logra con firmas y certificados.

IPSec trabaja de dos modos. El primero, transporte, que es el modo por default, y el segundo, túnel. El modo transporte provee de una conexión segura entre dos puntos, encapsulando sólo la parte útil del paquete IP, mientras que el modo túnel encapsula todo el paquete IP. El modo túnel tiene una funcionalidad parecida a la de una VPN, donde los paquetes IP son encapsulados enteramente dentro de otros y enviados al destino.

Authentication Header (AH) y *Encapsulating Security Payload* (ESP) son los dos protocolos principales a nivel de paquete usados por IPSec. Ellos autentican (AH) y cifran-autentican (ESP) la data en cada conexión.

- **AH** es usado para autenticar, pero no para encriptar. La autenticación del tráfico IP es realizado operando un *Hash-based message authentication code* sobre todos los campos del paquete IP, excluyendo todos aquellos que pueden ser modificados en el camino, como el TTL o el *header checksum*.
- **ESP** provee de cifrado y de una autenticación opcional.

Para poder establecer una conexión mediante IPSec se necesitan *Security Associations* (SA). Un SA es un conjunto de parámetros requeridos para establecer una conexión segura. Estos parámetros son el *Security Parameter Index* (SPI), la dirección IP de destino y el identificador del protocolo de seguridad. El SA es unidirecional y sólo puede ser usado para un protocolo, entonces se necesitan dos SAs para una comunicación direccional y dos o mas SAs para cada protocolo de seguridad (AH y ESP). Hay dos formas de configurar un SA: Manualmente; en donde se tiene que configurar cada nodo, y automáticamente; usando un *Internet Key Exchange* (IKE). La negociación IKE está compuesta de dos fases:

- El objetivo de la primera fase IKE es establecer un canal de comunicación seguro usando el algoritmo de intercambio de claves Diffie-Hellman para generar una clave de secreto compartido y así cifrar la comunicación IKE. La fase 1 opera tanto en modo principal como agresivo. El modo principal protege la identidad de los extremos, mientras que el modo agresivo no lo hace.
- En la segunda fase IKE, los extremos usan el canal seguro establecido en la primera fase para negociar una SA. La segunda fase opera sólo en modo rápido.

Algoritmos Usados

- **Algoritmos de Cifrado**
  - DES (Estándar de Cifrado de Datos): Usa una encryption key con una extensión de 56 bits. Ese es el más débil de los tres algoritmos.
  - 3DES (Triple-DES): Un algoritmo de cifrado basado en DES que utiliza el DES para cifrar los datos tres veces.
  - AES (Estándar de Cifrado Avanzado): El algoritmo de cifrado más fuerte que existe. Fireware puede utilizar encryption key de AES de los siguientes largos: 128, 192, o 256 bits.
- **Algoritmos de Autenticación**
  - HMAC-MD5 (Código de Autentificación de Mensaje Hash - Algoritmo de Resumen de Mensaje 5): MD5 produce un resumen de mensaje de 128 bits (16 bytes), que lo hace más rápido que SHA1 o SHA2. Éste es el algoritmo menos seguro.
  - HMAC-SHA1 (Código de Autentificación de Mensaje Hash - Secure Hash

Algorithm 1): SHA1 produce un resumen de mensaje de 160 bits (20 bytes). Aunque sea más lento que el MD5, ese archivo más grande es más fuerte contra los ataques de fuerza bruta.

- HMAC-SHA2 (Código de Autentificación de Mensaje Hash — Secure Hash Algorithm 2): SHA2 es más fuerte que SHA1 o MD5.

- **Algoritmo de Intercambio de Clave Diffie-Hellman**

  El algoritmo de intercambio de clave Diffie-Hellman (DH) es un método usado para que una clave de cifrado compartida esté disponible a dos entidades sin el intercambio de la clave. La clave de cifrado para los dos dispositivos es usada como una clave simétrica para encriptar datos. Solamente las dos partes involucradas en el intercambio de clave DH pueden deducir la clave compartida, y la clave nunca es enviada por cable. Un grupo de clave Diffie-Hellman es un grupo de números enteros usados para el intercambio de la clave Diffie-Hellman.

Hardware Criptográfico

Para acelerar los algoritmos criptográficos utilizados por IPsec, se usa hardware especializado en hacer operaciones criptográficas. Una variedad de hardware de cifrado está disponible y la selección de hardware depende de la aplicación. La mayoría de las implementaciones de hardware son naturaleza asíncrona; es decir, funcionan en paralelo con el procesador principal. Existen los siguientes tipos de hardware criptográfico.

- **System Cards**

  Esta categoría de hardware criptográfico generalmente viene en forma de PCI y está diseñado para su uso en servidores basados en PC. Proporciona operaciones criptográficas para IPsec, SSL y cifrado de archivos.

- **Security (Co)processors**

  Comúnmente llamados procesadores de seguridad o hardware aceleradores, son dispositivos que proveen de operaciones criptográficas vía bus de memoria o otro mecanismo de acceso similar. Estos dispositivos pueden utilizarse en una tarjeta del sistema o en un sistema con un procesador de red. Algunos ejemplos son HIFN, SafeNET y dispositivos Freescale MPC184/190.

- **Security-Enabled Processors**

  Son dispositivos que contienen el procesador principal y el procesador de seguridad en un *system-on-a-chip* (SOC). Esta integración de funcionalidad permite que la seguridad sea implementada de forma más rentable en dispositivos de bajo costo como enrutadores VPN.

Referencias

[1] APNIC eLearning, “IPSec Basics”

[2] IPSec Reference, StarOS Release 20, “Introduction to IP Segurity (IPSec)”

[3] S. Frankel Nist, S. Krishnan Ericsson, “IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap”, 2011.

[4] Fireware Help, “Acerca de los Algoritmos y Protocolos de IPSec”

[5] Lumpkin, Todd, and Kim Phillips, “Linux, IPsec, and Crypto Hardware Acceleration”, 2006.