Una arquitectura de seguridad para IP

Rafael Espinosa-García
Sistemas VLSI
respinosa@cs.cinvestav.mx
Tel: 5747-7001 ext. 6261

Guillermo Morales-Luna
Sección de Computación
gmorales@cs.cinvestav.mx
Tel: 5747-3759

CINVESTAV-IPN
Apartado Postal 14-740
México, D.F.

Introducción

El impresionante crecimiento de Internet y su correspondiente conectividad, además del advenimiento de nuevos servicios, ha propiciado que intrusos técnicamente avanzados consideren como un reto constante el emprender ataques de índole diversa que amenacen la integridad y la privacidad de redes de comunicación de datos en general. Por otro lado, el avance de la tecnología de comunicaciones y sus beneficios ha modificado el rechazo inicial de usuarios gubernamentales o de negocios a relegar en Internet elementos estratégicos de información. En particular el temor a intrusos anónimos provenientes de Internet está obligando a las organizaciones a considerar soluciones radicales tales como la separación entre redes de datos privadas (Intranets) y la red pública Internet. La segmentación obtenida se está constituyendo en un fuerte impedimento para lograr el concepto de una red Internet global, lo que establecería una conectividad fuertemente acoplada.

En 1994, el *Internet Architecture Board* (IAB) emitió el reporte "*Security in the Internet Architecture*" (*RFC 1636*), el cual establecía que Internet requería una mayor y mejor seguridad, además, identificaba las áreas claves que requerían mecanismos de seguridad. Entre las principales necesidades quedaron identificadas: el aseguramiento de la infraestructura de red, tanto del monitoreo como del control del tráfico no autorizado, y la protección del trafico usuario_final-usuario_final utilizando mecanismos de autentificación y de encriptamiento.

El protocolo *Internet Protocol*, IP, es uno de los más usados para la interconexión de redes tanto en ambientes académicos como corporativos, y naturalmente lo es también en la Internet pública. Su flexibilidad y sus poderosas capacidades lo han impuesto como un vehículo de interconectividad por un largo tiempo. La fuerza de IP radica en su facilidad y su flexibilidad para el envío de grandes volúmenes de información en pequeños datagramas a través de los diversos esquemas de enrutamiento.

Sin embargo, IP presenta ciertas debilidades. La forma en que el protocolo enruta los paquetes hace que las grandes redes IP sean vulnerables a ciertos riesgos bien conocidos de seguridad. Uno de ellos es el llamado *IP Spoofing*, en el cual un intruso ataca cambiando la dirección del paquete IP, haciéndolo aparecer como si éste se hubiese originado en otro lugar. Otro de tales ataques es la intromisión en una transmisión IP

mediante el uso de un analizador de protocolos, lo que permitiría hacer un seguimiento del tráfico en la red. Mencionamos como un último tipo de ataque a IP aquel realizado cuando el intruso irrumpe en una sesión establecida y se enmascara como si fuese una de las partes en esa comunicación.

Debido a que estas vulnerabilidades limitan y complican el uso de las grandes redes IP (incluyendo por supuesto a toda Internet) en comunicaciones altamente sensibles, un grupo internacional organizado bajo el *Internet Engineering Task Force* (IEFT) desarrolló el *IP Security* (IPSec) *protocol suite*, como un conjunto de extensiones para IP que ofrecen servicios de seguridad en el nivel de red (de acuerdo con el modelo de capas de ISO de OSI). La tecnología de IPSec se basa en la criptografía moderna, lo que garantiza, por un lado, la privacidad y, por otro, una autentificación fuerte de datos.

Las características de IPSec lo hacen único debido a que implementa seguridades en la capa *de red* más que en la *de aplicaciones*. En el pasado, otros grupos habían desarrollado métodos a nivel de aplicación para protección de comunicaciones, incluyendo esquemas tales como el *PGP/Web-of-Trust* para protección del correo electrónico. Mientras estos métodos son efectivos para resolver problemas de seguridad particulares, las soluciones que aportan se encuentran circunscritas a sus nichos especifícos. Dado que el protocolo IPSec asegura a la red por sí misma, se garantiza que las aplicaciones que se estén usando en la red sean, en efecto, seguras.

Existen ya numerosos productos que implementan IPSec. Sin embargo, también es cierto que no es necesariamente la elección correcta para una solución de seguridad para un administrador de red. Para ofrecer seguridad en el nivel de IP es necesario que IPSec sea parte del código de red en todas las plataformas participantes, incluyendo sistemas Windows NT, UNIX y Macintosh, pues de otra manera una aplicación dada podría fracasar al inetentar usar las funciones de seguridad del protocolo. Sin embargo, para una red virtual privada, IPSec ofrece, en efecto, las facilidades al nivel de la capa de red requeridas.

IPSec ofrece tres facilidades principales:

- una función de autentificación, referida como *Authentication Header* (AH),
- una función combinada de autentificación/encriptamiento llamada *Encapsulating Security Payload* (ESP), y
- una función de intercambio de llaves.

Para las redes virtuales privadas (VPN), tanto la autentificación como el encriptamiento son, por lo general, deseables, pues:

(1) aseguran que usuarios no autorizados no penetren en la VPN y
(2) aseguran que los mirones en Internet no puedan leer mensajes privados enviados sobre la VPN.

Ambas características son deseables y la mayoría de las implementaciones se adaptan más a ESP que a AH. La función de intercambio de llaves permite realizar esta función ya sea en forma manual o bien en forma automática.

Evidentemente, la aceptación genera-lizada de un IP seguro está propiciada por la necesidad de usuarios corporativos y gubernamentales para conectar sus infraestructuras WAN/LAN a Internet para

(1) el acceso a servicios de Internet y
(2) el uso de la Internet como una componente del sistema de transporte WAN.

Los usuarios requieren aislar sus redes y al mismo tiempo enviar y recibir tráfico sobre Internet. Los mecanismos de seguridad IP proporcionan la base para una estrategia de seguridad.

Debido a que los mecanismos de seguridad IP han sido definidos en forma independiente de su uso, ya sea con el IP, de uso mayoritario en la actualidad, o con IPv6 (*IP version 6*), la organización de estos mecanismos no depende del desarrollo de IPv6. Es pues altamente probable que se extienda el uso de las características de seguridad de IP aún antes de que IPv6 venga a ser más popular.

En el presente trabajo hacemos una retrospectiva acerca de las características y los beneficios de la arquitectura de *IP Security* (IPSec), sus mecanismos de operación y los productos ya disponibles en el mercado.

Beneficios de IPSec

Cuando se implementa IPSec en un *router*, éste provee una fuerte seguridad que puede ser aplicada a todo el tráfico que cruza el perímetro servido por el *router*. Por otro lado, IPSec está debajo de la capa *de transporte* (TCP, UDP), así pues resulta "transparente" para las aplicaciones. No hay necesidad de cambiarlas, ni desde el punto de vista del usuario ni del servidor cuando IPSec se incorpora al *router* o al *firewall*. También se tiene que IPSec puede ser "transparente" a los usuarios finales. Como una política general, puede asumirse que no es necesario involucrar a los usuarios en los mecanismos de seguridad. Finalmente, IPSec tiene la capacidad de ofrecer seguridad individual si ésta fuese indispensable. Tal característica es útil para empleados que accedan a la red desde el exterior vía telefónica. Además, es posible asegurar una subred virtual dentro de una organización para aplicaciones sensibles. En resumen, entre los beneficios de IPv6 mencionamos:

- herencia de niveles de seguridad, de *routers* a subredes,
- transparencia respecto a las aplicaciones,
- transparencia respecto a usuarios finales, y
- ofrecimiento de seguridad a nivel individual.

Estructura de IPSec

En agosto de 1995, el IETF publicó cinco documentos relacionados con la propuesta para estandarizar la capacidad de seguridad al nivel de toda Internet:

- *RFC 1825*: Descripción de la arquitectura de seguridad
- *RFC 1826*: Descripción del paquete de extensión para autentificación en IP
- *RFC 1828*: Especificación del mecanismo de autentificación
- *RFC 1827*: Descripción de paquete de extensión para encriptamiento en IP
- *RFC 1829*: Especificación del mecanismo de encriptamiento

Estas características son obligatorias en IPv6 y opcionales en IPv4. En ambos casos, la parte de seguridad se implementa mediante encabezados de extensión que siguen al encabezado principal de IP. El encabezado de extensión para autentificación es conocido como *Authenticacion Header* (AH) y para el caso de encriptamiento se la ha nombrado *Encapsulating Security Payload* (ESP).

Dentro del IETF, se estableció el *IP Security Protocol Working Group*, en donde se desarrolló la especificación completa de IPSec. Los documentos obtenidos se agruparon en siete categorías:

- *Architecture*: Establece los conceptos generales: requisitos de seguridad, definiciones y mecanismos caracte-rísticos de la tecnología de IPSec.
- *Encapsulating Security Payload* (ESP): Describe el formato del paquete y las

definiciones generales relacionadas para el uso de ESP para el encriptamiento de paquetes, y opcionalmente la autentificación.
- *Authentication Header* (AH): Describe el formato del paquete y las definiciones generales relacionadas para el uso de AH para la autentificación de paquetes, así como su algoritmo MAC (Message Authentication Code).
- *Encryption Algorithm*: Documentos que describen cómo los diversos algoritmos de encriptamiento son utilizados por ESP, tales como DES, Triple-DES, RC5, IDEA, CAST, BLOWFISH y RC4.
- *Authentication Algorithm*: Documentos que describen cómo los diversos algoritmos son usados por AH y por la opción de autentificación de ESP.
- *Key Management*: Documentos que describen los esquemas para administración de las llaves.
- *Domain of Interpretation* (DOI): Contiene parámetros necesarios para diversos documentos relacionados entre sí. Estos incluyen identificadores para algoritmos de autentificación y de encriptamiento aprobados, así como también parámetros operacionales tales como *tiempos de vigencia de llaves* (*key lifetime*).

Servicios IPSec

IPSec ofrece servicios de seguridad en la capa de IP habilitando un sistema para seleccionar protocolos de seguridad necesarios, determinar algoritmos a utilizar en los servicios y colocar en cualquier lugar las llaves criptográficas requeridas para cumplir con los servicios solicitados. Se utilizan dos protocolos para proveer seguridad: uno para autentificación, diseñado para el encabezado del protocolo AH, y otro combinado para autentificación / encriptamiento diseñado para el formato del paquete en el protocolo ESP. Los servicios proporcionados son:

- Control de acceso
- Integridad sin conexión
- Autentificación de origen
- Rechazo de paquetes retocados (como una forma de integridad secuencial parcial)
- Confidencialidad (encriptamiento)
- Confidencialidad limitada por el flujo del tráfico

Seguridad IP

La arquitectura de *Seguridad del Internet Protocol* conocida como *IP Security* es el esfuerzo más avanzado para estandarizar la seguridad en Internet. IP es el vehículo común para los protocolos de las capas más altas y en consecuencia es susceptible de enfrentar ataques severos, ya sea a la seguridad de los datos manejados por las aplicaciones y transportados por los protocolos de las capas más altas, como TCP (*Transmision Control Protocol*), o al comportamiento de la red en sí misma interviniendo los protocolos de control como ICMP (*Internet Control Protocol Message Protocol*) o BGP (*Border Gateway Protocol*). Tanto en la versión actual de IP (IPv4) como en el IP de la nueva generación (IPv6) es posible utilizar IPSec debido a la modificación retroactiva de los mecanismos de seguridad de IPv6 en IPV4.

IPSec puede usarse para proteger la capa de IP entre un par de sistemas finales o servidores, entre un par de sistemas intermedios, también conocidos como *gateways*, o entre un servidor y un *gateway* de seguridad. Un tal *gateway* permite el reenvío de paquetes en la capa de IP, y por tanto puede ser un *router*, un *firewall* o un servidor. Los protocolos de IPSec tienen las siguientes funciones de seguridad en la capa IP:

- autentificación de origen de datos,
- integridad de datos,
- detección de respuesta,
- confidencialidad de datos y

- control de acceso.

Suplementariamente a los mecanismos de seguridad individual implementados por estos servicios, IPSec cuenta con facilidades de administración para la negociación de servicios y de parámetros entre las partes comunicantes, así como también, para el intercambio de llaves criptográficas requeridas por los mecanismos de seguridad básicos, los cuales se diseñaron para no depender de los algoritmos criptográficos actuales y, en consecuencia, propiciar su posible evolución. No obstante, hay algoritmos por omisión definidos para cada servicio, lo cual facilita la interoperabilidad de los servicios.

La versión más reciente de IPSec consiste de las siguientes componentes:

- Dos protocolos de seguridad: *IP Authentication Header* (AH) y *IP Encapsulating Security Payload* (ESP) que aportan los mecanismos básicos de seguridad dentro de IP.
- *Security Associations* (SA) que especifican los servicios de seguridad y los parámetros negociados en cada trayectoria segura IP.
- Algoritmos para autentificación y para encriptamiento.

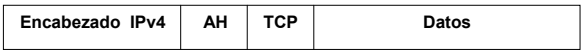
Tanto AH como ESP pueden ser aplicados ya sea en forma individual o en forma combinada. Cada protocolo puede, a su vez, ser operado en una de dos formas: *modo transporte* o *modo túnel*. En el modo transporte, los mecanismos de seguridad del protocolo se aplican sólo a las capas más altas de los datos y la información pertinente a la capa de operación cuando está contenida en el encabezado de IP el cual queda desprotegido, es decir, "abierto", "llano" o "plano". En modo túnel, tanto los datos de los protocolos de las capas superiores como el encabezado IP del datagrama IP son protegidos o "tuneleados" a través del encapsulamiento.

Una función crucial relacionada cercanamente a las componentes de IPSec antes mencionadas es la administración automática del material criptográfico transmitido y las SA's. El protocolo *Internet Security Association and Key Management* especifica las funciones de administración automática para las componentes de seguridad en la capa de IP.

Autentificación

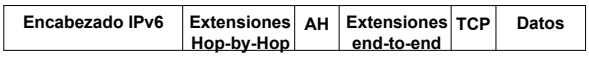
El encabezado de autentificación (*Authentication Header* -- AH) de IPSec, es un mecanismo que provee las funciones de una integridad fuerte y de autentificación para datagramas IP. La *integridad* garantiza que el datagrama no sea alterado en forma inesperada o maliciosa, y la *autentificación* verifica el origen del datagrama (nodo, usuario, red, etc.). AH solo no acepta toda forma de encriptamiento, por lo cual no puede proteger la confidencialidad de cualesquiera datos enviados sobre Internet. Más bien, AH está orientado a mejorar la seguridad en el Internet global en situaciones donde importar, exportar o usar encriptamiento puede ser ilegal o estar restringido por disposiciones de gobiernos locales. AH ha de estar libre de tales complicaciones, razón por la cual ofrece el servicio de autentificación de paquetes IP. Con esto se reduce la frecuencia de ataques basados en *IP spoofing*.

AH asume la forma de un encabezado colocado entre el encabezado de IPv4 o IPv6 y la siguiente trama del protocolo de la capa más alta, tales como TCP, UDP, ICMP, etc. La implementación de AH en IPv4 es opcional. El datagrama IP tiene un formato relativamente simple:



IPv4

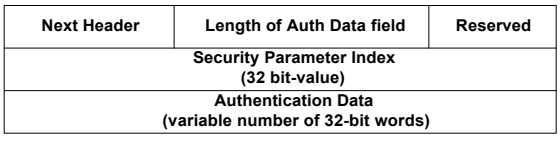
En cambio, la implementación de AH en IPv6 es obligatoria y el datagrama es más complejo. Dentro del datagrama, AH aparece después de los encabezados de IP, procesados en cada *hop*, y antes de los encabezados IP procesados sólo en el destino final. El siguiente diagrama muestra la posición de AH en el datagrama IPv6.



IPv6

IANA (*Internet Assigned Numbers Authority*) ha asignado el número de protocolo 51 a AH. Por tanto, el encabezado IP inmediatamente prece-dente al encabezado de AH debe contener el valor 51 en el campo *Next_Header* para IPv6 o en el campo *Next_Protocol* en IPv4.

AH ofrece mecanismos de integridad y autentificación realizando un *cálculo de compendio de mensajes* (*message digest calculation*) sobre el datagrama IP completo. Un *compendio de mensaje* es una transformación matemática especial, de un solo sentido, que crea una *huella digital* única del datagrama, representándolo así mediante un solo número mucho más pequeño. El resultado del algoritmo de compendio de mensaje se coloca en el campo *Authentication_Data* del encabezado AH. El formato completo del encabezado AH es pues el siguiente:



Authentication Header

El protocolo AH se ha diseñado pretendiendo que funcione con diversos algoritmos de autentificación, tanto con aquellos ya existentes como con los que han de desarrollarse en un futuro. IPSec DOI asigna un número único para cada algoritmo de autentificación, el cual sirve como identificador durante el proceso de negociación entre sistemas que se están comunicando. Se han definido dos algoritmos para autentificación y son considerados obligatorios de acuerdo con el estándar de IPSec: HMAC (*Hashed Message Authentication Code*)-MD5 (*Message Digest version 5*) y HMAC (*Hashed Message Authentication Code*)-SHA1 (*Secure Hash version 1*).

HMAC-MD5

El algoritmo MD5 es una función matemática de un solo sentido. Aplicado a un bloque de datos, éste produce una representación única de 128 bits de él. El resultado obtenido es una representación comprimida o codificada de un bloque más grande de datos. Cuando se usa de esta manera, MD5 garantiza sólo la integridad en los datos. Un mensaje codificado ha de ser sometido a un proceso de cálculo partiendo de un bloque de datos (como pueden ser datagramas IP) antes de que se envíe y otra vez después de que los datos hayan sido recibidos. Si los dos compendios calculados son iguales, entonces el bloque de datos no tuvo alteración alguna durante la transmisión (suponiendo que hubiese habido una transmisión maligna). El algoritmo MD5 se detalla en el *RFC 1321*.

La autenticidad puede ser garantizada mediante el uso de llaves secretas cuando se calcula el mensaje codificado. El método HMAC usa el algoritmo básico MD5 para calcular los mensajes codificados, pero opera en bloques de datos de 64 bytes que sirve, a su vez, como entrada de un bloque entero de datos. Este también usa una llave secreta (conocida sólo por los sistemas que se están

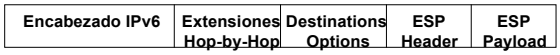
comunicando) cuando se realiza el cálculo de la codificación. HMAC se describe en detalle en el *RFC 2104*.

En un sistema de intercambio de datagramas utilizando HMAC-MD5, el emisor previamente intercambiará la llave secreta, para calcular primero una serie de compendios MD5 de 16 bits por cada bloque de 64 bytes del datagrama. La serie de valores formados por los compendios de 16 bytes se concatenan en un solo valor, el cual es colocado en el campo *Authentication_Data* del encabezado AH. El datagrama se envía al receptor, quien debe también conocer el valor de la llave secreta para calcular el mensaje codificado correcto y compararlo con el mensaje codificado recibido por autentificación. Si los valores coinciden, ha de concluirse que el datagrama no fue alterado durante su tránsito por la red, y además, éste fue enviado sólo por otro sistema compartiendo el conocimiento de la llave secreta. Hay que hacer notar que la utilidad de esta técnica se basa en la presunción de que sólo el verdadero emisor (y no un impostor) tiene conocimiento de la llave privada compartida.

Encriptamiento

El encabezado *Encapsulating Security Protocol* (ESP) realiza funciones de integridad y de confidencialidad para datagramas IP. Como ya lo hemos dicho, la integridad asegura que el datagrama no haya sido alterado en forma inesperada o maliciosa, y la confidencialidad asegura la privacidad de los datos usando técnicas criptográficas.

Para implementaciones IPv6, ESP toma la forma de un encabezado que es colocado después de todos los encabezados IP en el datagrama IP. A continuación se muestra su formato:



Hay que hacer notar los dos tipos de encabezados opcionales mostrados en el formato. Los encabezados *Hop-by-Hop* son procesados por sistemas intermedios (como *routers*) en cada *hop*. En tanto que, considerando los encabezados del campo *Destination,* éstos son sólo procesados por el sistema final. El encriptamiento de ESP no debe interferir con ninguna parte de los encabezados IP necesarios para la entrega correcta del paquete.

IANA (*Internet Assigned Numbers Authority*) ha designado el número de protocolo 50 para ESP. Esto significa que el encabezado IP inmediatamente precedente al encabezado ESP debe contener el valor de 50 en el campo *Next_Header* (en IPv6) o en el campo *Next_Protocol* (en IPv4).

El protocolo ESP, como AH, se diseñó para trabajar en dos modos: *túnel* y *transporte*. La diferencia radica en el contenido de la porción *ESP_Payload* del datagrama IP. En modo túnel, un datagrama completo se encapsula y se encripta dentro de *ESP_Payload*. Cuando se hace esto, las direcciones verdaderas IP, origen y destino, pueden ser ocultas como un mero dato transitando en Internet. Un uso típico de este modo es cuando se esconde un servidor o una topología durante una conexión *firewall-to-firewall* sobre una red virtual privada (VPN). En el modo transporte, en contraste, sólo la trama de los protocolos de las capas superiores (TCP, UDP, ICMP, etc.) se coloca en la porción encriptada *ESP_Payload* del datagrama. En este modo, ambas direcciones IP, origen y destino, así como también todos

los campos y opciones, se envían sin encriptar.

El protocolo ESP tiene un diseño flexible que le permite trabajar con diferentes algoritmos de encriptamiento (también nombradas *transformadas*). IPSec requiere de un algoritmo común por omisión. La *transformada DES-CBC*, puede ser usada en todas las implementaciones de ESP. Sin embargo, dos o más sistemas estableciendo una sesión IPSec pueden negociar el uso de una transformada alternativa. El documento *IPSec DOI* presenta una lista opcional de transformadas ESP. Aquí, entre los algoritmos opcionales están: Triple-DES, RC5, IDEA, CAST, BLOWFISH y RC4.

Procedimiento DES-CBC

DES (*Data Encryption Standard*) es un algoritmo de encriptamiento muy común. Publicado primero en 1977 por el Gobierno de los Estados Unidos de América, se usó para aplicaciones comerciales "no-clasificadas". Hoy día todas las patentes han expirado, y existen implementaciones gratuitas disponibles en el mundo. El estándar de IPSec para ESP requiere que todas las implementaciones realicen DES en modo CBC (*Cipher Block Chaining*) como tranformada por omisión. Sin embargo, su uso ciertamente no es obligatorio. Todo usuario u organización es libre de elegir otras transformadas de encriptamiento, o bien de plano no usar encriptamiento alguno. Tal flexibilidad es particularmente importante dada la reglamentación, desde el punto de vista jurídico, existente en cada país acerca del uso y la exportación de criptografía doméstica.

DES-CBC, tal como se especifica para ESP, trabaja ejecutando una operación matemática sobre bloques de datos de 8 bytes que comprimen ya sea un datagrama completo (modo túnel) o la trama del protocolo de la siguiente capa superior (modo transporte). DES-CBC reemplaza bloques de 8 bytes de datos no encriptados (texto plano) con bloques de 8 bytes de datos encriptados (texto cifrado). Esta propiedad de transformación facilita las funciones de encriptar/desencriptar una ráfaga (*stream*) de datos. Un valor aleatorio, o *vector de inicialización* (IV), de 8 bytes se usa para encriptar el primer bloque del texto plano y asegurar así la aleatoriedad entre mensajes que pueden comenzar con la misma información de texto plano.

La característica principal de encriptamiento de DES-CBC es una llave idéntica secreta compartida entre las partes comunicantes. Es, propiamente dicho, un *algoritmo criptográfico simétrico*. La llave usada por el emisor para encriptar los datos es la única llave que puede ser usada por el receptor para desencriptar los datos. Por tanto, el uso efectivo de DES-CBC para privacidad de datos depende de la misma llave secreta compartida entre las partes que se están comunicando, y, naturalmente, ha de ser protegida para no ser descubierta por los intrusos. La longitud de la llave especificada para DES-CBC usada dentro de ESP es de 56 bits.

El protocolo ISAKMP

El protocolo *Internet Security Association and Key Management* (ISAKMP) se basa en el concepto central de una asociación de seguridad (SA). Esta última es un acuerdo de seguridad unidireccional entre los sistemas que se están comunicando que especifican qué tan segura es una conexión que será establecida. SA contiene todos los parámetros necesarios para definir completamente el acuerdo de seguridad tales como: autentificación, algoritmos de encriptamiento, longitudes de llaves y tiempo de vigencia de las llaves. Todos los parámetros SA son organizados dentro de

una estructura llamada *Security Parameter Index* (SPI). Una SA es negociada para cada protocolo de seguridad utilizada entre los protocolos de los sistemas interconectados, dos sistemas pueden tener múltiples SA establecidas.

El establecimiento de SA's entre los sistemas se efectúa en dos fases: primero, una ISAKMP-SA es negociada entre los sistemas (tales como dos servidores ISAKMP). El ISAKMP se utiliza para proteger el tráfico entre los sistemas durante la segunda fase de negociación de los protocolos SA. Todos los protocolos que no sean ISAKMP-SA's han de ser considerados protocolos SA's (como por ejemplo, una AH-SA o una ESP-SA). El protocolo ISAKMP se diseñó para ofrecer seguridad en todas las capas del protocolo, no sólo en la capa de IP y de sus protocolos asociados AH y ESP. Sin embargo, también es posible para otros protocolos (SSL, TLS, OSPF, etc.) usar ISAKMP para establecer sus propias SA's. Cada protocolo de seguridad subsecuente o servicio usado por los sistemas que se comuniquen tendrá su propia SA y su correspondiente SPI. IANA ha asignado el puerto UDP 500 para uso del protocolo ISAKMP.

El protocolo Oakley

El establecer la primera fase de ISAKMP-SA involucra el intercambio de llaves autentificadas entre la comunicación de ambos sistemas para proteger el tráfico subsecuente y la negociación de los protocolos SA's. El protocolo *Oakley Key Determination* es un mecanismo usado para realizar este intercambio seguro. Oakley usa el algoritmo de intercambio de llaves de Diffie-Hellman (D-H), que es una técnica criptográfica de intercambio de llave pública que permite a cada sistema generar una llave secreta única en forma independiente basado en el conocimiento de cada una de las otras llaves públicas. La norma de ISAKMP requiere que las llaves públicas usadas para establecer ISAKMP-SA sean autentificadas mediante firmas digitales. ISAKMP no establece algoritmo alguno de firma en particular ni una *autoridad certificadora* (CA), mas sin embargo, a instancias de las partes, permite a los sistemas indicar cuáles CA's se aceptarán. A través de la implementación de Oakley, ISAKMP tiene un mecanismo para la identificación de tipos de certificados, de CA's aceptadas y de intercambio de certificados entre sistemas. Una vez que las llaves públicas D-H son intercambiadas y autentificadas y de que una llave secreta haya sido generada, los sistemas que están comunicados pueden establecer una IPSec-SA que caracteriza el uso subsecuente de los protocolos de seguridad AH y ESP.

Administración de llaves

La parte de administración de llaves de IPSec involucra la determinación y la administración de llaves secretas. Un requisito usual es el uso de cuatro llaves para comunicación entre dos aplicaciones: se transmite y se recibe pares de llaves tanto para AH como para ESP. Existen dos mecanismos para la administración de llaves:

- *Manual*: El administrador del sistema lo configura manualmente con sus propias llaves y con las llaves de otros sistemas con los que ha de comunicarse. Este método es práctico para un medio ambiente relativamente estático y pequeño.
- *Automático*: Se habilita la creación de llaves para un sistema en base a la demanda de SA's y se facilita el uso de llaves en un gran sistema distribuido con una configuración evolucionante.

El protocolo que administra automáticamente las llaves en IPSec se denomina

ISAKMP/Oakley y consiste de los elementos siguientes:

- *Oakley Key Determination Protocol*: Oakley es un protocolo de intercambio de llaves basado en el algoritmo Diffie-Hellman, ofreciendo una mayor seguridad. Oakley es genérico dentro del sistema y no tiene formato específico.
- *Internet Security Association and Key Management Protocol*: ISAKMP tiene un marco de referencia para la administración de llaves en Internet y cumple con protocolos específicos, incluyendo elementos como formatos para la negociación de atributos de seguridad.

ISAKMP por sí mismo no impone un algoritmo especifico para intercambio de llaves; más bien, ISAKMP consiste de un conjunto de mensajes típicos que habilitan el uso de una variedad de algoritmos de intercambio de llaves.

IPSec DOI

El documento *DOI* de normas para IPSec especifica todos los parámetros asociados con los protocolos AH y ESP, y los asigna como identificadores únicos. Este documento sirve como base de datos de valores para ser referenciados durante la negociación IPSec SA

IP layer security vs session layer security

IPSec y SSL son tecnologías complementarias cuando el tráfico se restringe a la "web", es decir, a HTTP (*HyperText Transfer Protocol*). SSL es pertinente, presuponiendo que los navegadores y los servidores de "web" ya tienen incluido SSL, naturalmente. Cuando el tráfico no puede ser restringido sólo a HTTP, y se deben incluir aplicaciones como Telnet, FTP, NFS (*Network File System*), servicios de directorio, aplicaciones de bases de datos, audio y video en tiempo real, entonces es necesario usar el protocolo IPSec.

Conclusiones

IPSec es una arquitectura de seguridad integrada existente para IP, incluyendo protocolos de seguridad cubriendo varios servicios, así como protocolos para la administración común de asociaciones de seguridad e intercambio de llaves. La seguridad puede ser provista en las capas superiores usadas por IPv4 o IPv6 como mecanismos básicos de transporte. Además, para proveer conexiones seguras que acomoden los requisitos específicos de las aplicaciones, el trabajo de la seguridad de la capa de transporte define un protocolo de seguridad inmediatamente debajo de la capa de aplicación. Basándose en la implementación de productos usados ampliamente, la versión actual de este protocolo consiste de una arquitectura independiente en donde se incluyen sus propias funciones de administración de seguridad.

La necesidad de seguridad es aún más fuerte para el control de red y las funciones de administración que las responsables de mantener la conectividad sobre la red global. Los protocolos de enrutamiento en IPv4 fueron extendidos recientemente con mecanismos de autentificación aislados. Sin embargo, el soporte a estas extensiones y su integración con el núcleo de IPSec son débiles aún. En IPv6, los protocolos de enrutamiento confiarán en la seguridad de IPSec como la mayoría de los protocolos que utilizan la capa de IP. La administración de red es crucial para su operación en un área donde la seguridad criptográfica es demasiado débil a pesar de numerosos intentos por incluir opciones de seguridad en versiones recientes de SNMP (*Simple Network Management Protocol*). En sentido inverso, DNS (*Domain Name System*) posee una arquitectura bien definida para extensiones de seguridad para autentificar su base de datos y las transacciones de cada usuario.

Cuando la seguridad se enfoca como un problema de red global, un asunto importante lo es la administración de sus servicios. Debido a la complejidad de las interacciones entre diversos mecanismos de seguridad implementados en los protocolos y la necesidad de contar con una configuración automática de ellos, ISAKMP y Oakley ofrecen una solución adecuada para la administración de asociaciones de seguridad y el intercambio de llaves compartidas con los protocolos IPSec. Otros protocolos, como RIP y OSPF para enrutamiento y TLS, probablemente se integren al núcleo de la arquitectura y hagan uso de ISAKMP y de Oakley. La administración de llave pública está siendo explorada por diversos proveedores, sin embargo aún no se ha consensuado una solución común.

Referencias

Molva, Refik, Internet security architecture, *Computer Networks*, Vol. 31, No. 8, april 1999, Elsevier.

Stallings, William, IP Security, *The Internet Protocol Journal*, Vol. 3, No. 1, march 2000, CISCO.

Cheng, P.C., Garay, J.A., Herzberg, A. and Krawczyk, H., A security architecture for the Internet Protocol, *IBM System Journal,* Vol. 37, No. 1, 1998, IBM.

Murhammer, M.W., Atakan, O., Bretz, S., Pugh, L.R., Suzuki, K., and Wood, D.H., *TCP/IP Tutorial and Technical Overview*, october 1998, IBM.

Allard, J., and Nygren, S., IPSec Safety First and interoperability, *Data Communications*, june 1999, CMP.