Grupo de Trabajo en Red
Request for Comments: 2406
Obsoletes: 1827
Categoría: Pila de Estándares

S. Kent
BBN Corp
R. Atkinson
@Home Network

Noviembre 1998

Traducción al castellano:
Agosto 2005

Hugo Adrian Francisconi <adrianfrancisconi@yahoo.com.ar>

Carga de Seguridad IP Encapsulada (ESP)

Estado de este documento

Este documento especifica un protocolo de Internet en vías de estandarización para la comunidad de Internet y solicita debate y sugerencias para mejorarlo. Por favor, remítase a la edición actual de "Estándares de Protocolos Oficiales de Internet" (STD 1) para conocer el estado de estandarización y status de este protocolo. La distribución de este memorándum es ilimitada.

Aviso de Copyright

Lista de contenido

1. Introducción

La cabecera de Carga de Seguridad Encapsulada (ESP) esta diseñada para proporcionar un conjunto de servicios de seguridad en IPv4 y en IPv6. ESP puede ser aplicado solo, o en combinación con la Cabecera de Autentificación (AH) [KA97b], o en forma anidada, por ejemplo, a través del uso del modo túnel (véase "Arquitectura de Seguridad para IP" [KA97a], de aquí en adelante designado como documento de la Arquitectura de Seguridad). Los servicios de seguridad pueden ser suministrados a comunicaciones, entre un par de hosts, o entre un par de security gateway (SG), o entre security gateway y un host. Para más detalles de cómo se usa ESP y AH en varios ambientes de red, ver el documento de la Arquitectura de Seguridad [KA97a].

La cabecera ESP se inserta antes que la cabecera IP y después que la cabecera de protocolo de capa superior (en modo transporte) o después de una cabecera IP encapsulada (en modo túnel). Estos modos se describen más detalladamente debajo.

ESP es usado para proporcionar confidencialidad, autentificación del origen de los datos, integridad sin conexión, un servicio de anti-replay (una forma parcial de integrabilidad de secuencia) y confidencialidad limitada del flujo de trafico. El conjunto de servicios proporcionados depende de las opciones seleccionadas al momento del establecimiento de la Asociación de Seguridad (SA) y de dónde esté localizada la implementación. La confidencialidad puede ser seleccionada independientemente del resto de los servicios. No obstante el uso de la confidencialidad sin integridad/autentificación (en ESP o en AH) puede subordinar trafico hacia ciertos tipos de

ataques activos que podrían socavar el servicio de confidencialidad (ver [Bel96]). La autentificación del origen de los datos y la integridad sin conexión son servicios que están unidos (de aquí en adelante a ambos servicios se los denominará como "autentificación") y son ofrecidos como una opción junto con la confidencialidad (opcional). El servicio de anti-replay puede ser seleccionado únicamente si la autentificación del origen de los datos es seleccionado, y esta elección esta supeditada solamente al albedrío del receptor. (Aunque el valor por defecto exige que el emisor incremente el Número de Secuencia usado para el anti-replay, el servicio es efectivo solamente si el receptor controla el Número de Secuencia.) La confidencialidad del flujo de tráfico requiere de la selección del modo túnel, y es más efectiva si esta implementada en una security gateway donde la agregación de tráfico puede encubrir patrones verdaderos del origen y del destinatario. Observe que aunque la confidencialidad y la autentificación son opcionales, al menos una de ellas debe ser seleccionada.

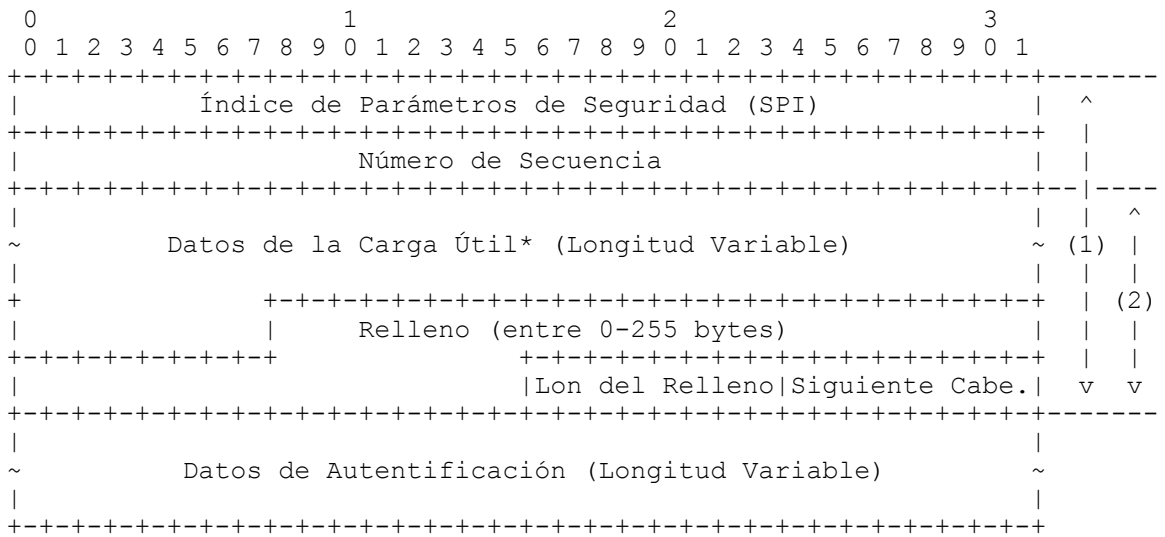
Se asume que el lector está familiarizado con los términos y los

conceptos descriptos en el documento de la Arquitectura de seguridad. Particularmente, el lector debe estar familiarizado con las definiciones de servicios de seguridad ofrecidas para AH y ESP, el concepto de Asociaciones de Seguridad (SA), las formas en las cuales ESP se puede utilizar conjuntamente con AH, y las diversas opciones de administración de clave disponibles para AH y ESP (con respecto al último punto, las opciones requeridas actualmente para manejo de claves tanto para AH como para ESP es en modo manual y en modo automatizado por medio de IKE [HC98].)

Las palabras DEBE, NO DEBE, REQUERIDO, PODER, NO PODER, DEBERÍA, NO DEBERÍA, RECOMENDADO, PUEDE y OPCIONAL, cuando aparezcan en este documento, deben interpretarse como se describe en el RFC 2119 [Bra97].

2. Formato del Paquete de la Carga de Seguridad Encapsulada

La cabecera del protocolo (IPv4, IPv6, o de Extensión) inmediatamente antes de la cabecera de ESP contendrá el valor 50 en su Protocolo (IPv4) o en el campo Siguiente Cabecera (de IPv6, o de Extensión) [STD-2].



(1) Alcance de la Autentificación

(2) Alcance de la Confidencialidad

* Si se incluye en el campo Carga útil los datos de sincronización criptográficos, por ejemplo, un Vector de Inicialización (IV, ver Sección 2.3), usualmente no esta encriptado, aunque a menudo se lo hace referencia como parte del texto cifrado.

Las secciones subsiguientes definen el formato de los campos en la cabecera. "Opcional" significa que el campo es omitido si la opción no es seleccionada, es decir, no esta presente ni en el paquete ni como trasmitido ni como formateado para el cálculo del Valor de Comprobación de Integridad (ICV, ver Sección 3.7). Si una opción es o no seleccionada es definido como parte del establecimiento de la Asociación de Seguridad (SA). Así, el formato de los paquetes ESP para una SA dada es fijo, para la duración de la SA. En cambio, los campos "obligatorios" están siempre presentes en el formato del paquete ESP, para todas las SAs.

2.1 Índice de Parámetros de Seguridad (SPI)

El SPI es un valor arbitrario de 32 bits que, conjuntamente con la dirección de destino IP y el protocolo de seguridad (ESP), identifican unívocamente a la Asociación de Seguridad para este datagrama. El conjunto de valores de SPI en el rango de 1 a 255 está

reservado por la IANA (Internet Assigned Numbers Authority) para uso futuro; un valor reservado de SPI no será destinado normalmente por el IANA a menos que el uso del valor destinado de SPI se especifique en un RFC. Este es seleccionado por el sistema de destino sobre el establecimiento de una SA (véase el documento de la Arquitectura de Seguridad para más detalles). El campo SPI es obligatorio.

El valor de SPI cero (0) esta reservado para usarse localmente, las implementaciones no deben trasmitir este valor por la red. Por ejemplo, una implementación de administración de clave PUEDE utilizar el valor cero de SPI para denotar que "No Existe Asociación de seguridad" durante el período en el cual la implementación IPsec ha solicitado a la entidad administradora de claves que se establezca una nueva SA, pero la SA todavía no se ha establecido.

2.2 Número de Secuencia

Campo de 32 bits sin signo que contiene un valor crecientes y único del contador (del número de secuencia). Es obligatorio y debe estar siempre presente incluso si el receptor elige no habilitar el servicio de anti-replay para una SA específica. El procesamiento del campo Número de Secuencia esta a criterio del receptor, es decir, el emisor DEBE transmitir siempre este campo, pero el receptor no necesita actuar sobre él (véase la discusión de la Verificación del

Número de Secuencia en "Procesamiento de Paquetes Entrantes" en la sección posterior).

El contador del emisor y del receptor se inicializan a cero (0) cuando se establece una SA. (El primer paquete que se envíe bajo esa SA tendrá el Número de Secuencia 1; vea la Sección 3.3.3 para más detalles de cómo se genera el Número de Secuencia.) Si se habilita el anti-replay (por defecto), la transmisión del Número de Secuencia nunca debe permitir que el Número de Secuencia retorne a cero. Por ende, el contador del emisor y del receptor DEBEN ser resetiados (para el establecimiento de una nueva SA y de esta manera también una nueva clave) antes de que se trasmitan 2^32 paquetes sobre una SA.

2.3 Datos de la Carga Útil

Los Datos de la Carga Útil es un campo de longitud variable que contiene los datos descriptos por el campo Siguiente Cabecera. El campo Datos de la Carga Útil es obligatorio y cuya longitud es un número de bytes enteros. Si el algoritmo usado para encriptar a la carga útil requiere datos de sincronización criptográficos, por ejemplo, de un Vector de Inicialización (IV), estos datos SE PUEDEN llevar explícitamente en el campo Carga Útil. Cualquier algoritmo de encriptación que requiera tales datos explícitos, un paquete previo

de sincronización de los datos DEBERÁ indicar la longitud, la estructura para tales datos, y la localización de estos datos como parte de la especificación del RFC del algoritmo que se utiliza con ESP. Si tales datos de sincronización son implícitos, el algoritmo para derivar los datos DEBE ser parte del RFC.

Note que en cuanto a la certeza de alinear el (verdadero) texto cifrado en presencia de un IV:

- Para alguno de los modos de operación basados en IV, el receptor trata el IV como el comienzo del texto cifrado, introduciéndolo dentro del algoritmo directamente. En estos modos, la alineación del comienzo del (verdadero) texto cifrado no es asunto del receptor.

- En algunos casos, el receptor lee el IV por separado del texto cifrado. En estos casos, la especificación del algoritmo DEBE tratar la forma de alinear el (verdadero) texto cifrado.

2.4 Relleno (para la Encriptación)

Varios factores requieren o motivan el uso del campo Relleno.

- Si se emplea un algoritmo de encriptación que requiere que el texto plano sea un múltiplo de un cierto número de bytes, por ejemplo, el tamaño de bloque de un bloque cifrado, el campo Relleno es usado para rellenar el texto plano (el cual consta de los Datos de la Carga Útil, y los campos Longitud del Relleno y Siguiente Cabecera, así como también del Relleno) para el tamaño requerido por el algoritmo.

- El relleno también puede ser requerido, independientemente de los requisitos del algoritmo de encriptación, para asegurarse de que el texto cifrado resultante termine en un límite de 4 bytes. Específicamente, los campos Longitud del Relleno y Siguiente Cabecera deben estar alineados correctamente dentro de una palabra de 4 bytes, según lo ilustrado en la figura del formato del paquete ESP, para asegurarse de que el campo Datos de Autentificación (si está presente) esté alineado en un límite de 4 bytes.

- Más allá del relleno requerido para el algoritmo o por las razones de alineación citadas arriba, se puede utilizar para encubrir la longitud real de la carga, en respaldo de la confidencialidad (parcial) del flujo de tráfico. Sin

embargo, la inclusión de tal relleno adicional tiene implicaciones adversas en el ancho de banda y su uso bebe ser emprendido con cautela.

El emisor PUEDE agregar de 0 a 255 bytes de relleno. La inclusión del campo Relleno en un paquete ESP es opcional, pero todas las implementaciones DEBEN soportar la generación y el uso del relleno.

a. Con el fin de asegurarse de que los bits que se encriptarán sean múltiplo del tamaño del bloque del algoritmo (primer punto de arriba), el cómputo del relleno se aplica a los campos Datos de la Carga Útil no incluyendo los del IV, al campo Longitud del Relleno, y al campo Siguiente Cabecera.

b. Para los propósitos de asegurarse de que los Datos de Autentificación estén alineados en un límite de 4 bytes (segundo punto de arriba), el cómputo del relleno se aplica a los campos Datos de la Carga Útil incluyendo los del IV, al campo Longitud del Relleno, y al campo Siguiente Cabecera.

Si son necesarios los bytes de relleno pero el algoritmo de encriptación no especifica el contenido del relleno, entonces el proceso que se describe a continuación (proceso por defecto) DEBE ser utilizado. Los bytes de Relleno se inicializan con una serie de (bytes sin signo) de valores de números enteros. El primer byte del relleno añadido al texto plano se lo numera como 1, con los bytes subsiguientes de relleno formado por una secuencia sucesiva creciente: 1, 2, 3,... Cuando se emplea este esquema de relleno, el receptor DEBERÍA examinar el campo Relleno. (Este esquema fue seleccionado debido a su simplicidad relativa, fácil implementación en hardware, y porque ofrece protección limitada contra ciertas formas de ataques de "copiar y pegar" en ausencia de otras medidas de integridad, si el receptor controla los valores del relleno sobre la desencriptación.)

Cualquier algoritmo de encriptación que requiera Relleno con excepción del valor por defecto descripto arriba, DEBE definir el contenido del Relleno (por ejemplo, ceros o datos aleatorios) y cualquier proceso requerido por el receptor de estos bytes de Relleno debe estar especificado en un RFC que especifique como se usa el algoritmo con ESP. En tales circunstancias, el contenido del campo Relleno será determinado por el algoritmo de encriptación y el modo seleccionado y definido en el RFC correspondiente del algoritmo. El RFC relevante del algoritmo PUEDE especificar que un receptor DEBE examinar el campo Relleno o que un receptor DEBE informar al emisor cómo el receptor manejará el campo Relleno.

2.5 Longitud del Relleno

El campo Longitud del Relleno indica el número de bytes de relleno inmediatamente precedentes a este campo. El rango de valores válidos es de 0 a 255 bytes, donde un valor de cero indica que no hay bytes de Relleno presentes. El campo Longitud del Relleno es obligatorio.

2.6 Siguiente Cabecera

La Siguiente Cabecera es un campo de 8 bits que identifica el tipo de datos contenidos en el campo Datos de la Carga Útil, por ejemplo, una cabecera de extensión IPv6 o un identificador de protocolo de capa superior. El valor de este campo se elige del conjunto de Números de Protocolo IP definidos en el más resiente RFC de "Números Asignados" [STD-2] por la Autoridad de Números de Asignación de Internet (IANA).

2.7 Datos de Autentificación

El campo Datos de Autentificación es de longitud variable y contiene el Valor de Comprobación de Integridad (ICV) calculado sobre el paquete ESP menos, los Datos de Autentificación. La longitud del campo es especificada por la función de autentificación seleccionada. El campo Datos de Autentificación es opcional, y se incluye solamente si el servicio de autentificación se ha seleccionado para la SA en cuestión. La especificación del algoritmo de autentificación DEBE especificar la longitud del ICV y las reglas de comparación y los pasos para el procesamiento de validación.

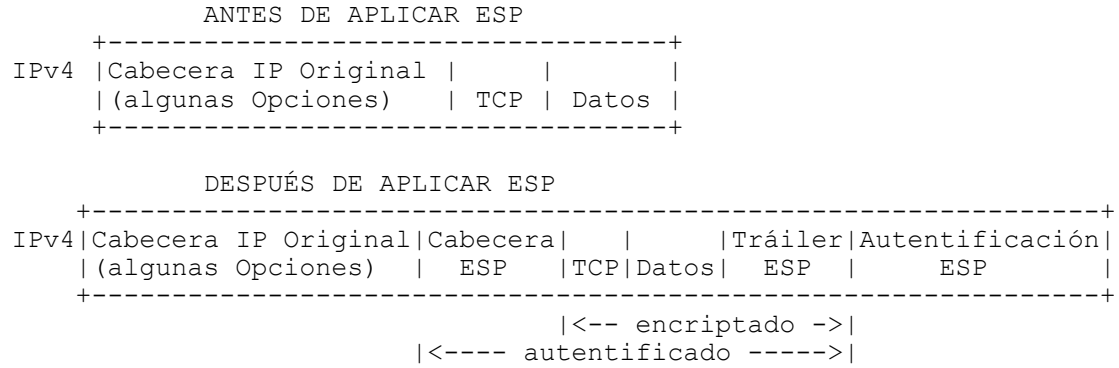
3. Procesamiento del Protocolo Encapsulación de Seguridad

3.1 Localización de la Cabecera ESP

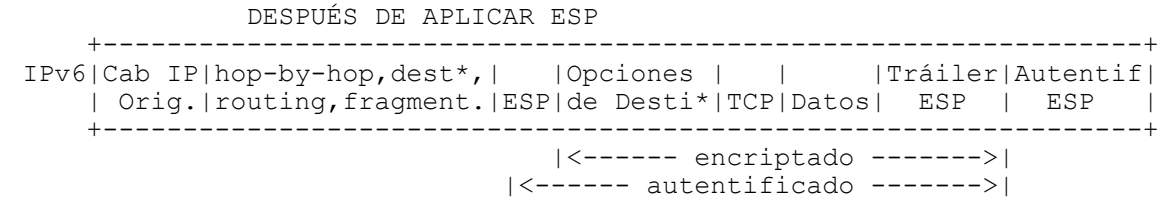
Como AH, ESP puede ser empleado de dos maneras: modo transporte o

modo túnel. El primer modo es aplicable solamente a implementaciones host y proporciona la protección para los protocolos de capa superiores, pero no a la cabecera IP. (En este modo, observe que para las implementaciones "bump-in-the-stack" (BITS) o "bump-in-the-wire" (BITW), según lo definido en el documento de la Arquitectura de Seguridad, los fragmentos IP entrantes y salientes pueden requerir que una implementación IPsec realice un reensamblaje/fragmentación IP adicional a fin de que ambos cumplan con las especificaciones y proporcionen un soporte IPsec transparente. Especial cuidado se requiere para realizar tales operaciones dentro de estas implementaciones cuando múltiples interfaces se están usando.)

En modo transporte, ESP se inserta después de la cabecera IP y antes del protocolo de capa superior, por ejemplo, TCP, UDP, ICMP, etc. o antes que cualquier otra cabecera IPsec que se haya insertado. En el contexto de IPv4, esto se traduce en la colocación de ESP después de la cabecera IP (y de cualquiera de las opciones que contenga), pero antes del protocolo de capa superior. (Observe que el término modo "transporte" no debería ser mal interpretado restringiendo su uso solamente a TCP y UDP. Por ejemplo, un mensaje ICMP SE PUEDE enviar usando modo "transporte" o modo "túnel".) El diagrama siguiente ilustra el "antes y el después" de ESP en modo transporte ubicado en un paquete típico de IPv4. (El "tráiler de ESP" incluye los campos: Relleno, Longitud del Relleno, y Siguiente Cabecera.)



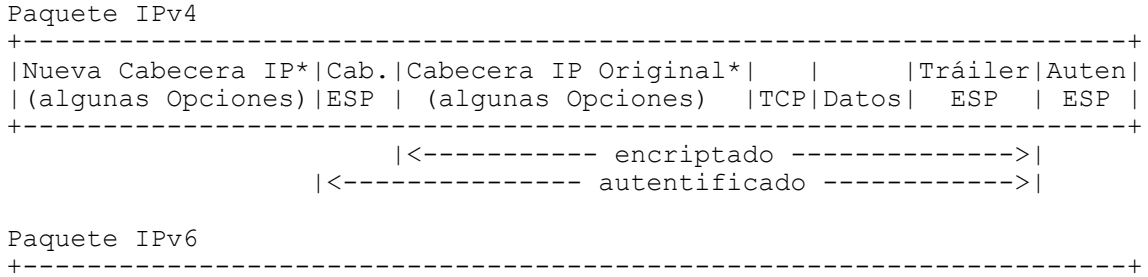
En el contexto de IPv6, ESP se ve como carga útil extremo a extremo, y por ende debe aparecer después de las cabeceras de extensión de salto-por-salto (hop-by-hop), ruteo (routing) y de fragmentación. La cabecera de extensión opciones de destino(s) podría aparecer antes o después de la cabecera ESP dependiendo de la semántica deseada. Sin embargo, puesto que ESP protege solamente a los campos que están después de la cabecera ESP, generalmente puede ser deseable colocar la cabecera opciones de destino(s) después de la cabecera ESP. El diagrama siguiente ilustra a ESP en modo transporte ubicado en un paquete típico de IPv6.

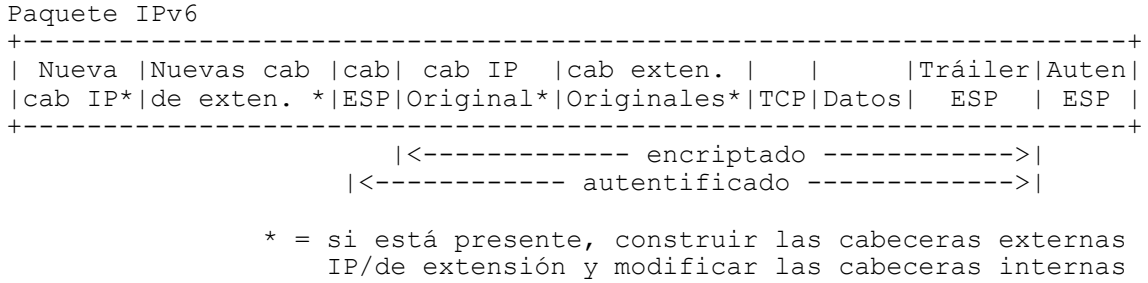


* = si esta presente, podría estar antes de ESP, después de ESP, o en ambos

Las cabeceras ESP y AH se pueden combinar en varios modos. El documento de la Arquitectura de Seguridad de IPsec describe las combinaciones de asociaciones de seguridad que deben ser soportadas.

ESP en modo túnel puede ser empleado en hosts o security gateways. Cuando se implementa ESP en una security gateway (para proteger el tráfico en tránsito del suscriptor), se debe utilizar el modo túnel. En modo túnel, la cabecera IP "interna" lleva las últimas direcciones de origen y destino, mientras que una cabecera IP "externa" puede contener direcciones IP distintas, por ejemplo, las direcciones de las security gateways. En modo túnel, ESP protege a todo el paquete IP interno, incluyendo toda la cabecera IP interna. La posición de ESP en modo túnel, concerniente a la cabecera externa IP, es igual que para ESP en modo transporte. El diagrama siguiente ilustra ESP en modo túnel ubicado en un paquete típico de IPv4 y de IPv6.





* = si está presente, construir las cabeceras externas IP/de extensión y modificar las cabeceras internas IP/de extensión según lo discutido posteriormente.

3.2 Algoritmos

Los algoritmos que se deben implementar obligatoriamente se describen en la Sección 5, "Requerimientos de Conformidad". Otros algoritmos PUEDEN ser soportados. Observe que aunque la confidencialidad y la autentificación son opcionales, por lo menos uno de estos servicios DEBE ser seleccionado, por lo tanto, ambos algoritmos NO DEBEN ser simultáneamente NULL.

3.2.1 Algoritmos de Encriptación

El algoritmo de encriptación empleado es especificado por la SA. ESP esta diseñado para usarse con algoritmos de encriptación simétricos. Debido a que los paquetes IP pueden llegar en desorden, cada paquete debe llevar necesariamente algún tipo de dato para permitir que el receptor establezca la sincronización criptográfica para la desencriptación. Estos datos se pueden llevar explícitamente en el campo carga útil, por ejemplo, un IV (como se describió anteriormente), o los datos pueden ser derivados de la cabecera del paquete. Puesto que ESP establece normas para el relleno del texto plano, los algoritmos de encriptación empleados con ESP pueden exhibir características de encriptación en modo bloque o de flujo (secuencial). Observe que puesto que la encriptación (confidencialidad) es opcional, este algoritmo puede ser "NULL".

3.2.2 Algoritmos de Autentificación

El algoritmo de autentificación empleado para el cálculo del ICV esta especificado por la SA. Para la comunicaciones punto-a-punto, los

algoritmos de autentificación más aptos incluyen claves con Código de Autentificación de Mensaje (MACs) basados en algoritmos de encriptación simétricos (por ejemplo, DES) o funciones hash unidireccionales (por ejemplo, MD5 o SHA-1). Para comunicación multicast, los algoritmos hash unidireccionales combinados con algoritmos de firmas asimétricas son apropiados, aunque las consideraciones de funcionamiento y de espacio actual imposibilitan el uso de tales algoritmos. Observe que puesto que la autentificación es opcional, este algoritmo puede ser "NULL".

3.3 Procesamiento de Paquetes Salientes

En modo transporte, el emisor encapsula la información del protocolo de la capa superior en la cabecera/tráiler de ESP, y mantiene la cabecera IP especificada (y cualquiera de las cabeceras IP de extensión en el contexto de IPv6). En modo túnel, la cabecera/extensiones IP externas e internas se pueden interrelacionar

de diversas formas. La construcción de las cabecera/extensiones IP externas realizada durante el proceso de la encapsulación se describe en el documento de la Arquitectura de Seguridad. Si se requiere más de una cabecera/extensión IPsec debido a la política de seguridad, el orden de aplicación de las cabeceras de seguridad SE DEBE definir en la política de seguridad.

3.3.1 Buscando la Asociación de Seguridad

ESP se aplica a un paquete saliente solamente después que una implementación IPsec determine que el paquete está asociado con una SA la cual requiere el procesamiento de ESP. El proceso de determinar qué, si existe alguno, procesamiento IPsec se aplica al tráfico saliente, se describe en el documento de la Arquitectura de Seguridad.

3.3.2 Encriptación del Paquete

En esta sección, hablamos del término encriptación siempre aplicado a las implicaciones del formato. Esto se hace con la comprensión que no se ofrece "confidencialidad" usando el algoritmo de encriptación NULL. Por consiguiente, el emisor:

1. Encapsula (dentro del campo Carga Útil de ESP):
   - Para el modo transporte: solo la información primitiva del protocolo de la capa superior.
   - Para el modo túnel: el datagrama IP primitivo entero.
2. Agregar cualquier relleno necesario.
3. Encriptar el resultado (Datos de la Carga Útil, Relleno, Longitud del Relleno, y Siguiente Cabecera) usando la clave, el algoritmo de encriptación, el modo del algoritmo indicado por la SA y los datos de sincronización criptográficos (si hay).
   - Si los datos de sincronización criptográficos son explícitos, por ejemplo, un IV, es indicado, estos se ingresan en el algoritmo de encriptación según la especificación del algoritmo y se colocan en el campo Carga Útil.
   - Si los datos de sincronización criptográficos son implícitos, por ejemplo, un IV, es indicado, estos se construyen y se ingresan en el algoritmo de encriptación según la especificación del algoritmo.

Los pasos exactos para la construcción de la cabecera IP externa dependen del modo (transporte o túnel) y se describen en el documento de la Arquitectura de Seguridad.

Si se selecciona la autentificación, la encriptación se realiza primero, antes que la autentificación, y la encriptación no abarca el campo Datos de Autentificación. Este orden de procesamiento facilita la rápida detección y rechazo de paquetes re-enviados o falsos para el receptor, antes de desencriptar el paquete, por lo tanto reduciendo potencialmente el impacto de ataques de denegación de servicio. También permite la posibilidad de procesamiento en paralelo de paquetes en el receptor, es decir, la desencriptación puede ocurrir paralelamente a la autentificación. Observe que debido a que los Datos de Autentificación no están protegidos por la encriptación, un algoritmo de autentificación de claves debe ser empleado para calcular el ICV.

3.3.3 Generación del Número de Secuencia

El contador del emisor es inicializado a cero (0) cuando se establece una SA. El emisor incrementa el Número de Secuencia para esta SA e inserta el nuevo valor dentro del Campo Número de Secuencia. Así, el primer paquete enviado usando una SA dada tendrá un valor de Número de Secuencia de 1.

Si se habilita el anti-replay (por defecto), el emisor controla para asegurarse que el contador no ha completado un ciclo antes de insertar el nuevo valor en el campo Número de Secuencia. Es decir, el emisor NO DEBE enviar un paquete en una SA, si al hacerlo haría que el Número de Secuencia complete un ciclo. Una tentativa de transmitir un paquete que resultaría en un desbordamiento del Número de Secuencia es un evento auditable. (Observe que este método de administración del Número de Secuencia no requiere el uso de la aritmética modular.)

El emisor asume que el anti-replay es habilitado por defecto, a menos que sea notificado de otra cosa por el receptor (véase la Sección 3.4.3). Así, si el contador ha completado un ciclo, el emisor establecerá una nueva SA y una clave (a menos que la SA haya sido configurada con administración manual de claves).

Si el anti-replay esta deshabilitado, el emisor no necesita monitorear o volver a cero el contador, por ejemplo, en el caso de administración manual de claves (véase la Sección 5). Sin embargo, el emisor incrementa el contador y cuando alcanza el valor máximo, el contador vuelve otra vez a cero.

3.3.4 Cálculo del Valor de Comprobación de Integridad (ICV)

Si la autentificación es seleccionada para la SA, el emisor calcula el ICV sobre el paquete ESP menos los Datos de Autentificación. Así el SPI, el Número de Secuencia, los Datos de la Carga Útil, el Relleno (si esta presente), la Longitud del Relleno, y la Siguiente Cabecera son abarcados por el cálculo del ICV. Observe que los últimos 4 campos estarán en forma de texto cifrado, puesto que la encriptación se realiza antes de la autentificación.

Para algunos algoritmos de autentificación, la cadena de byte sobre la cual se calcula el ICV debe ser un múltiplo de un tamaño de bloque especificado por el algoritmo. Si la longitud de esta cadena de bytes no corresponde con los requisitos del tamaño de bloque para el algoritmo, el relleno implícito DEBE ser añadido al final del paquete ESP, (después del campo Siguiente Cabecera) antes del cálculo del ICV. Los octetos de relleno DEBEN tener un valor de cero. El tamaño del bloque (y por lo tanto la longitud del relleno) es especificado en la especificación del algoritmo. Este relleno no es transmitido con el paquete. Observe que MD5 y SHA-1 son vistos como que tienen un tamaño de bloque de 1 octeto debido a sus convenciones internas de relleno.

3.3.5 Fragmentación

Si se requiere, la fragmentación se realiza después del procesamiento ESP dentro de una implementación de IPsec. Así, en ESP en modo transporte se aplica solamente a datagramas IP enteros (no a fragmentos IP). Un paquete al cual se le ha aplicado ESP puede ser fragmentado por routers en ruta, y tales fragmentos se deben volver a reensamblar antes de que se lleve a cabo el procesamiento de ESP en el receptor. En modo túnel, ESP se aplica a un paquete IP, el cual la carga útil puede ser un paquete IP fragmentado. Por ejemplo, en un security gateway o en implementaciones IPsec BITS o BITW (según lo definido en el documento de la Arquitectura de Seguridad) se puede aplicar ESP en modo túnel a tales fragmentos.

NOTA: Para el modo transporte: Según lo mencionado al principio de la Sección 3.1, las implementaciones BITS y BITW puede que primero tengan que volver a reensamblar el paquete fragmentado por la capa IP local, después aplicar IPsec, y luego fragmentar los paquetes resultantes.

NOTA: Para IPv6: Para las implementaciones BITS y BITW, será necesario recorrer a través de todas las cabeceras de extensión para determinar si hay una cabecera de fragmentación y por lo tanto que el paquete necesita reensamblarse antes de realizar el procesamiento IPsec.

3.4 Procesamiento de Paquetes Entrantes

3.4.1 Reensamblaje

Si se requiere, el reensamblaje se realiza antes del procesamiento de ESP. Si un paquete brindado a ESP para procesamiento parece ser un fragmento IP, es decir, el campo de desplazamiento (OFFSET) es diferente a cero o la bandera de MAS FRAGMENTOS (MORE FRAGMENTS) está en uno, el receptor DEBE desechar el paquete; esto es un evento auditable. La entrada del registro de auditoría para este evento DEBERÍA incluir el valor del SPI, Fecha/Hora, Dirección de Origen, Dirección de Destino, Número de Secuencia y (En Ipv6) el Identificador de Flujo (Flow ID).

Nota: Para el reensamblaje del paquete, IPv4 NO requiere que el campo DESPLAZAMIENTO (OFFSET) sea cero o que este en cero la bandera de MAS FRAGMENTOS. Para que un paquete reensamblado pueda ser procesado por IPsec (contrariamente a descartar un aparente fragmento), el código IP debe hacer dos cosas después de reensamblar un paquete.

3.4.2 Buscando la Asociación de Seguridad

Al recibir un paquete (reensamblado) conteniendo una Cabecera ESP, el receptor determina la SA (unidireccional) apropiada, basándose en la dirección IP de destino, protocolo de seguridad (ESP), y el SPI. (Este proceso se describe más detalladamente en el documento de la Arquitectura de Seguridad.) La SA indica si se controlará el campo Número de Secuencia, si el campo Datos de Autentificación debería estar presente, y especificará los algoritmos y claves que se emplearán para la desencriptación y el cálculo del ICV (si son aplicados).

Si no existe ninguna SA válida para esta sesión (por ejemplo, el receptor no tiene ninguna clave), el receptor DEBE desechar el paquete; esto es un evento auditable. La entrada del registro de auditoría para este evento DEBERÍA incluir el valor del SPI, Fecha/Hora, Dirección de Origen, Dirección de Destino, Número de Secuencia, y (en IPv6) el Identificador de Flujo del texto plano.

3.4.3 Verificación del Número de Secuencia

Todas las implementaciones ESP DEBEN soportar el servicio de anti-replay, aunque su uso puede estar habilitado o deshabilitado por el receptor sobre la base de una SA. Este servicio NO DEBE ser habilitado si no esta habilitado el servicio de autentificación para esa SA, puesto que de otra forma el campo Número de Secuencia no tendrá protección de integridad. (Observe que no hay provisiones para

administrar los valores de Número de Secuencia transmitidos entre múltiples emisores que dirigen el tráfico a una única SA (independientemente de que si la dirección de destino es unicast, broadcast, o multicast). Así el servicio de anti-replay NO DEBERÍA ser usado en ambientes múlti-emisores que empleen una única SA.)

Si el receptor no habilita el anti-replay para una SA, no se realizarán comprobaciones salientes en el Número de Secuencia. Sin embargo, desde la perspectiva del emisor el valor por defecto es asumir que el anti-replay esta habilitado en el receptor. Para evitar que el emisor haga un monitoreo innecesario del número de secuencia y el establecimiento de una SA (ver Sección 3.3.3), si un protocolo de establecimiento de SA tal como IKE se emplea, el receptor DEBERÍA notificar al emisor, durante el establecimiento de una SA, si el receptor no proporcionará la protección anti-replay.

Si el receptor tiene habilitado el servicio de anti-replay para esta SA, el contador de recepción de paquetes para la SA, se debe inicializar en cero cuando la SA es establecida. Para cada paquete recibido, el receptor DEBE verificar que el paquete contiene un Número de Secuencia que no es igual al Número de Secuencia de ningún otro paquete recibido durante la vida de esa SA. Este DEBERÍA ser el primer control de ESP aplicado a un paquete después de que haya sido correspondido a una SA, para acelerar el rechazo de paquetes duplicados.

Los paquetes duplicados son rechazados a través del uso de una ventana de recepción deslizable. (La forma de implementar la ventana es un tema local, pero el siguiente texto describe la funcionalidad que la implementación debe tener.) Un tamaño de ventana mínimo de 32 DEBE ser soportado; pero un tamaño de ventana de 64 es más aconsejable y DEBERÍA ser empleado como valor por defecto. Otro tamaño de ventana (más grande que el mínimo) PUEDE ser elegido por el receptor. El receptor no notifica al emisor del tamaño de la ventana.

El lado "Derecho" de la ventana representa el valor de Número de Secuencia más alto autentificado y recibido en esta SA. Los paquetes que contienen Números de Secuencias menores que el lado "izquierdo" de la ventana son rechazados. Los paquetes que caen dentro de la ventana son controlados con una lista de paquetes recibidos dentro de la ventana. Un modo eficiente de realizar este control, basado en el uso de una máscara de bits (bit mask), se describe en el documento de la Arquitectura de Seguridad.

Si el paquete recibido cae dentro de la ventana y es nuevo, o si el paquete esta a la derecha de la ventana, el receptor procede con la verificación del ICV. Si la verificación ICV falla, el datagrama IP

recibido no es válido y el receptor DEBE descartar el paquete. Esto es un evento auditable. La entrada del registro de auditoría para este evento DEBERÍA incluir el valor del SPI, fecha/hora recibido, Dirección de Origen, Dirección de Destino, Número de Secuencia, y (en IPv6) el Identificador de Flujo. La ventana de recepción es actualizada solo si la verificación del ICV tiene éxito.

DISCUSIÓN:

Observe que si el paquete esta dentro de la ventana y es nuevo, o si esta fuera de la ventana en el lado "derecho", el receptor DEBE autentificar el paquete antes de actualizar el valor de la ventana de Número de Secuencia.

3.4.4 Verificación del Valor de Comprobación de Integridad

Si la autentificación a sido seleccionada, el receptor calcula el ICV sobre el paquete ESP menos los Datos de Autentificación usando el algoritmo de autentificación especificado y verifica que es el mismo que el ICV incluido en el campo Datos de Autentificación del paquete. Los detalles del cálculo se proporcionan debajo.

Si el ICV calculado y recibido concuerdan, el datagrama es válido, y es aceptado. Si el control falla, el receptor debe descartar el datagrama IP recibido porque no es válido; esto es un evento auditadle. Los datos del registro de auditoría deberían incluir el valor del SPI, fecha/hora recibido, Dirección de Origen, Dirección de Destino, Número de Secuencia, y (en IPv6) el Identificador de Flujo del texto plano.

DISCUSIÓN:

Comience por quitar y guardar el valor ICV (campo Datos de Autentificación). Luego controle la longitud total del paquete ESP menos los Datos de Autentificación. Si se requiere relleno implícito, basado en el tamaño del bloque del algoritmo de autentificación se agregan los bytes de relleno con valor cero al final del paquete ESP directamente después del campo Siguiente Cabecera. Realice el cálculo del ICV y compare el resultado con el valor guardado, usando las reglas de comparación definidas en las especificaciones del algoritmo. (Por ejemplo, si una firma digital y un hash unidireccional se utilizan para el cálculo del ICV, el proceso de correspondencia es más complejo.)

3.4.5 Desencriptación del Paquete

Como en la Sección 3.3.2 "Encriptación de Paquetes", hablamos aquí en términos de encriptación que son siempre utilizados debido a las implicaciones del formato. Esto se hace con la comprensión de que la "confidencialidad" no es ofrecida usando el algoritmo de encriptación NULL. Por consiguiente el receptor:

1. Desencripta los Datos de la Carga Útil de ESP, el Relleno, la Longitud del Relleno, y Siguiente Cabecera, usando la clave, el algoritmo de encriptación, el modo del algoritmo y datos de sincronización criptográficos (si existen), indicados por la SA.
   - Si los datos de sincronización criptográficos son explicitos, por ejemplo, un IV, es indicado, se toman del campo Carga Útil y se coloca en el algoritmo de desencriptación según la especificación del algoritmo.
   - Si los datos de sincronización criptográficos son implícitos, por ejemplo, un IV, es indicado, una versión local de IV es construida y es colocada en el algoritmo de desencriptación según la especificación del algoritmo.
2. Procesar cualquier relleno según lo especificado en la especificación del algoritmo de encriptación. Si se a empleado el esquema de relleno de valor por defecto (ver la Sección 2.4) el receptor DEBERÍA examinar el campo Relleno antes de quitar el relleno y antes de pasar los datos desencriptados a la siguiente capa.
3. Reconstruir el datagrama IP original de:
   - Para el modo trasporte: cabecera IP original más la información del protocolo original de la capa superior dentro del campo Carga Útil de ESP.
   - Para el modo túnel: la cabecera IP del túnel más el datagrama IP entero dentro del campo Carga Útil de ESP.

Los pasos exactos para reconstruir el datagrama original dependen del modo (trasporte o túnel) y están descriptos en el documento de la Arquitectura de Seguridad. Como mínimo, en el contexto de IPv6 el receptor DEBERÍA asegurarse que los datos desencriptados estén alineados a 8 bytes, para facilitar el procesamiento realizado por el protocolo identificado en el campo Siguiente Cabecera.

Si la autentificación a sido seleccionada, la verificación y la desencriptación pueden realizarse en serie o en paralelo. Para realizarla en serie, la verificación del ICV DEBERÍA realizarse primero. Si se realiza en paralelo, la verificación debe ser completada antes que el paquete desencriptado pase a un proceso posterior. El orden del proceso facilita una rápida detección y

rechazo de paquetes reenviados o falsos para el receptor, antes de desencriptar el paquete, por lo tanto reduciendo potencialmente el impacto de ataques de denegación de servicio. Observe que si el receptor realiza la desencriptación en paralelo con la autentificación, se debe tener cuidado para evitar posibles condiciones con relación al acceso de paquetes y a la reconstrucción del paquete desencriptado.

Observe que existe varias causas por las que la desencriptación puede "fallar":

a. La SA seleccionada puede no ser la correcta: La SA puede ser mal seleccionada debido a tampering con los campos SPI, dirección de destino, o tipo de protocolo IPsec. Tales errores, si asocian el paquete a otra SA existente, serán indistinguibles de un paquete corrompido, (caso c). Tampering con el SPI puede ser detectado por medio del uso de la autentificación. Sin embargo, una mala correspondencia con la SA podría aún ocurrir debido a tampering con el campo Dirección IP de Destino o el campo tipo de protocolo IPsec.

b. La longitud del relleno o los valores del relleno pueden ser erróneos: longitud del relleno y valores del relleno deficientes pueden ser detectados independientemente del uso de la autentificación.

c. El paquete ESP encriptado podría ser corrompido: Esto puede ser detectado si la autentificación es seleccionada para la SA.

En el caso (a) o (c), el resultado erróneo de la operación de desencriptación (datagrama IP o capa de trasporte no valida) no será necesariamente detectado por IPsec, y es responsabilidad del procesamiento del siguiente protocolo.

4. Auditoría

No todos los sistemas que implementan ESP implementarán auditoría. Sin embargo, si ESP es incorporado a un sistema que soporta auditoría, la implementación ESP debe también soportar auditoría y debe permitirle a un administrador de sistema habilitar o deshabilitar la auditoría para ESP. Para la mayoría la granularidad de la auditoría es un tema local. Sin embargo, varios eventos auditadles se identifican en esta especificación y para cada uno de estos eventos un conjunto mínimo de información debería ser incluido en el registro de auditoría definido. Información adicional también puede ser incluida en el registro de auditoría para cada uno de estos

eventos, y los eventos adicionales, no explícitamente exigidos en esta especificación, también pueden resultar en entradas del registro de auditoría. No hay requisito para el receptor de trasmitir ningún mensaje al emisor pretendido en respuesta a la detección de un evento auditadle, debido al potencial de inducir la Denegación de Servicio a través de tal acción.

5. Requerimiento de Conformidad

Las implementaciones que demandan conformidad deben implementar la síntesis ESP y el proceso descriptos aquí y deben cumplir con todos los requisitos del documento de la Arquitectura de Seguridad. Si la clave usada para calcular un ICV es distribuida manualmente, la correcta provisión del servicio anti-replay requerirá el correcto estado del contador en el emisor, hasta que la clave es reemplazada y no habría probablemente disponibilidad automatizada de recuperación si el desbordamiento del contador fuera inminente. Así, una implementación no DEBERÍA proporcionar este servicio en conjunto con SAs que generan claves manualmente. Una implementación ESP debe soportar e implementar obligatoriamente los siguientes algoritmos:

- DES en modo CBC [MD97]
- HMAC con MD5 [MG97a]
- HMAC con SHA-1 [MG97b]
- Algoritmo de Autentificación NULL
- Algoritmo de Encriptación NULL

Puesto que la encriptación y la autentificación son opcionales, el soporte para los dos algoritmos "NULL" se requieren para mantener la consistencia con el modo en que estos servicios son negociados. Observe que a pesar de que la autentificación y la encriptación pueden ser NULL, estos NO DEBEN ser conjuntamente ambos NULL.

6. Consideraciones de Seguridad

La seguridad es esencial para el diseño de este protocolo y las consideraciones de seguridad invaden la especificación. Aspectos de seguridad adicionales con relación al uso del protocolo IPsec están discutidos en el documento de la Arquitectura de Seguridad.

7. Diferencias con el RFC 1827

Este documento se diferencia del RFC 1827 [ATK95] de varias formas significativas. La mayor diferencia es que, este documento intenta especificar un marco y un contexto completo para ESP, mientras que el RFC 1827 proporciona una cubierta que fue completada a través de la definición de trasformaciones. El crecimiento combinatorio de trasformaciones motivó la reformulación de la especificación de ESP

como un documento mas completo, con opciones para servicios de seguridad que puedes ser ofrecidos en el contexto de ESP. Así, los campos previamente definidos en documentos de transformación son ahora parte de esta base de especificación ESP. Por ejemplo, los campos necesarios para soportar autentificación (y anti-replay) están ahora definidos aquí, aun cuando la provisión de este servicio es opcional. Los campos usados para soportar el relleno para la encriptación, y para la identificación del siguiente protocolo, esta ahora definidos aquí. El procesamiento del paquete de acuerdo con la definición de estos campos también esta incluido en este documento.

Agradecimientos

Muchos de los conceptos contenidos en esta especificación fueron derivados de o influenciados por el protocolo de seguridad SP3 del gobierno de USA, ISO/IEC's NLSP, el protocolo de seguridad propuesto swIPe [SDNS, ISO, IB93].

Por más de tres años, este documento a evolucionado a lo largo de múltiples versiones e interacciones. Durante este tiempo, mucha gente a contribuido con ideas significativa y energía al proceso y al documento mismo. Los autores quisieran agradecer a Karen Seo por proporcionar ayuda extensiva en la revisión, edición, investigación de fondo, coordinación de la versión de esta especificación. Los autores quisieran también agradecer a los miembros del grupo de trabajo de IPsec y IPng con especial mención a los esfuerzos de (en orden alfabético): Steve Bellovin, Steve Deering, Phil Karn, Perry Metzger, David Mihelcic, Hilarie Orman, Norman Shulman, William Simpson and Nina Yuan.

Referencias

[ATK95] Atkinson, R., "IP Encapsulating Security Payload (ESP)", RFC 1827, August 1995.

[Bel96] Steven M. Bellovin, "Problem Areas for the IP Security Protocols", Proceedings of the Sixth Usenix Unix Security Symposium, July, 1996.

[Bra97] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

[HC98] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[IB93] John Ioannidis & Matt Blaze, "Architecture and Implementation of Network-layer Security Under Unix", Proceedings of the USENIX Security Symposium, Santa Clara, CA, October 1993.

[ISO92] ISO/IEC JTC1/SC6, Network Layer Security Protocol, ISO-IEC DIS 11577, International Standards Organisation, Geneva, Switzerland, 29 November 1992.

[KA97a] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[KA97b] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[MD97] Madson, C., and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[MG97a] Madson, C., and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

[MG97b] Madson, C., and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[STD-2] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994. See also: http://www.iana.org/numbers.html

[SDNS89] SDNS Secure Data Network System, Security Protocol 3, SP3, Document SDN.301, Revision 1.5, 15 May 1989, as published in NIST Publication NIST-IR-90-4250, February 1990.

Renuncia de Responsabilidades

Las opiniones y la especificación expresadas en este documento son la de los autores y no son necesariamente las de sus empleadores. Los autores y sus empleadores niegan específicamente la responsabilidad de cualquier problema que se presenta de la puesta en práctica o implementación correcta o incorrecta de uso de este diseño.

Información de los Autores

Stephen Kent
BBN Corporation
70 Fawcett Street
Cambridge, MA 02140
USA

Phone: +1 (617) 873-3988
EMail: kent@bbn.com

Randall Atkinson
@Home Network
425 Broadway,
Redwood City, CA 94063
USA

Phone: +1 (415) 569-5000
EMail: rja@corp.home.net

Declaración de Copyright Completa

LA INFORMACIÓN AQUÍ EXPUESTA NO INFRINGIRÁ NINGÚN DERECHO O GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO ESPECIFICO.

Notas del Traductor

Las Siguientes palabras no han sido traducidas y su significado es el siguiente:

. Tampering: violación de seguridad en la comunicación, en la cual la información en transito es cambiada o reemplazada y es enviada hacia el receptor. (Definición extraída del Diccionario de IBM Corp.)

Los Términos que aparecen entre "[]" que no sean referencias reflejan la palabra/s en inglés de las palabra/s que se encuentran (en español) a la izquierda, debido a que NO ESTOY SEGURO de que sea la correcta traducción del término o simplemente para que no se pierda el VERDADERO sentido del texto.

Esta presente traducción fue realizada por Hugo Adrian Francisconi para mi tarjado de tesis de "Ingeniero en Electrónico" en la Facultad U.T.N. (Universidad Nacional Tecnología) Regional Mendoza - Argentina. Si le interesa IPsec y quieres saber más podes bajarte mi trabajo de tesis, "IPsec en Ambientes IPv4 e IPv6" de http://codarec6.frm.utn.edu.ar, para el cual traduje varios RFCs al español relacionados con IPsec. Cualquier sugerencia debate o comentario sobre este presente tema o traducción será bien recibida en adrianfrancisconi@yahoo.com.ar

Se a realizado el máximo esfuerzo para hacer de esta traducción sea tan completa y precisa como sea posible, pero no se ofrece ninguna garantía implícita de adecuación a un fin en particular. La información se suministra "tal como está". El traductor no será responsable ante cualquier persona o entidad con respecto a cualquier pérdida o daño que pudiera resultar emergente de la información contenida en está traducción.

Derechos de Copyright Sobre Esta Traducción

Esta traducción tiene los mismos derechos que le RFC correspondiente traducido, con el aditamento de que cualquier persona que extraiga TOTAL o PARCIALMENTE esta traducción deberá hacer mención de esta presente nota de copyright y de los datos del traductor.

Datos del Traductor

Nombre y Apellido del Traductor: Hugo Adrian Francisconi
Domicilio: Carril Godoy Cruz 2801, Villa Nueva-Guay Mallen-Mendoza-
Argentina
Código Postal: 5500
Tel: 054-0261-4455427
E-mail: adrianfrancisconi@yahoo.com.ar