Grupo de Trabajo en Red
Request for Comments: 2402
Categoría: Pila de Estándares

S. Kent
BBN Corp
R. Atkinson
Noviembre 1998

Traducción al castellano:
Hugo Adrian Francisconi

Agosto 2005
<adrianfrancisconi@yahoo.com.ar>

Cabecera de Autentificación IP

Estado de este documento

Aviso de Copyright

Lista de contenido

1. Introducción

La Cabecera de Autentificación IP (Athentication Header - AH) se usa para proporcionar integridad sin conexión y autenticación del origen de datos para datagramas IP ("autentificación" a partir de ahora), y para proporcionar protección contra reenvíos. Este último servicio es opcional y puede seleccionarse una vez que se ha establecido la Asociación de Seguridad (SA). (Aunque se establece por defecto que el emisor incremente el Número de Secuencia usado en el anti-replay, el servicio es efectivo solamente si el receptor controla el Número de Secuencia.) HA proporciona autentificación a las partes de la cabecera IP que se les pueda brindar este servicio, así como también a los datos de los protocolos de las capas superiores. Sin embargo, algunos campos de la cabecera IP pueden cambiar durante el transporte, y el valor de estos campos, cuando el paquete llega al receptor, puede que no sea previsible para el emisor. Los valores de tales campos no pueden ser protegidos por AH. Así la protección proporcionada a la cabecera IP por AH se proporciona a fragmentos.

AH se puede aplicar solo, o en combinación con la Carga de Seguridad Encapsulada IP (ESP) [KA97b], o a través de la modalidad anidada usando el modo túnel (véase "Arquitectura de Seguridad para IP"

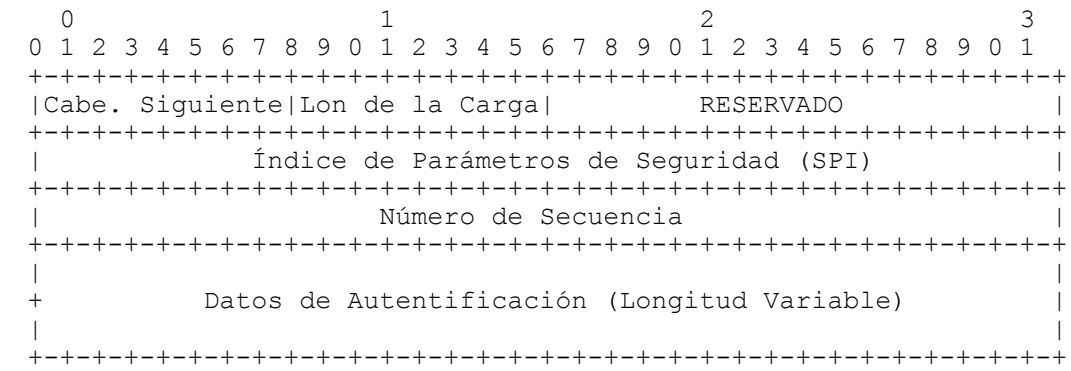
[KA97a], de aquí en adelante designado como documento de la Arquitectura de Seguridad). Los servicios de seguridad pueden ser suministrados a comunicaciones, entre un par de hosts, o entre un par de security gateway (SG), o entre security gateway y un host. ESP puede ser usado para proporcionar los mismos servicios de seguridad, y también para proporcionar un servicio de confidencialidad (encriptación). La diferencia principal entre la autentificación proporcionada por ESP y la de AH es la extensión de la cobertura. Específicamente, ESP no protege ninguno de los campos de la cabecera IP a menos que esos campos sean encapsulados por ESP (en modo túnel). Para más detalles en cómo utilizar AH y ESP en varios ambientes de red, vea el documento de la Arquitectura de Seguridad [KA97a].

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 AH se puede utilizar conjuntamente con ESP, y las diversas opciones de administración de clave disponibles para AH y ESP (con respecto al último punto, las opciones requeridas actualmente para el manejo de claves tanto para AH como para ESP son el modo manual y en el 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 de la cabecera de Autentificación

La cabecera del protocolo (IPv4, IPv6, o de Extensiones) inmediatamente antes de la cabecera de AH contendrá el valor 51 en el Protocolo (IPV4) o en el campo Cabecera Siguiente (de Extensión, en IPv6) [STD-2].



Las siguientes subsecciones definen los campos que comprenden el formato de AH. Todos los campos descriptos aquí son obligatorios, es decir, están siempre presentes en el formato de AH y se incluyen en el cálculo del Valor de Comprobación de Integridad (Integrity Check Value - ICV), (ver las Sección 2.6 y 3.3.3).

2.1 Cabecera Siguiente

La Cabecera Siguiente es un campo de 8 bits que identifica el tipo de carga siguiente después de la Cabecera de Autentificación. 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).

2.2 Longitud de la Carga

Este campo de 8 bits especifica la longitud de AH en palabras de 32 bit (en unidades de 4 byte), menos "2". (Todas las cabeceras de extensión de IPv6, según el RFC 1883, codifican el campo "Longitud de la Cabecera de Extensión" primero restando uno (palabra de 64-bit) a la longitud de la cabecera (medido en palabras de 64-bit). AH es una cabecera de extensión IPv6. Sin embargo, puesto que su longitud se mide en palabras de 32 bit, la "longitud de la carga" es calculada restando 2 (palabras de 32 bit).) En el caso "estándar" de un valor de autentificación de 96 bits positivos divididos en 3 palabras de 32 bits de tamaño fijo, este campo tendrá una longitud de "4". Un algoritmo de autentificación "NULL" puede ser usado solamente para propósitos de depuración (puesta a punto del sistema). Su uso daría lugar a un valor "1" para este campo en IPv4 o "2" en IPv6, puesto que no habría Datos de Autentificación en el correspondiente campo (ver Sección 3.3.3.2.1 "Carga de Datos de Autentificación").

2.3 Reservado

Este campo de 16 bits esta reservado para uso futuro. DEBE ser fijado a "cero." (Observe que el valor está incluido en el cálculo de los datos de autentificación, pero es ignorado por el receptor.).

2.4 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 (AH), identifican unívocamente a la Asociación de Seguridad para este datagrama. El conjunto de valores de SPI en el rango de 1 a 255 están reservados por la IANA 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 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.

2.5 Número de Secuencia

Campo de 32 bits sin signo que contiene un valor creciente y único del contador (de 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 0 cuando se establece una SA. (El primer paquete que se envíe bajo esa SA tendrá el Número de Secuencia 1; vea la Sección 3.3.2 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.

2.6 Datos de Autentificación

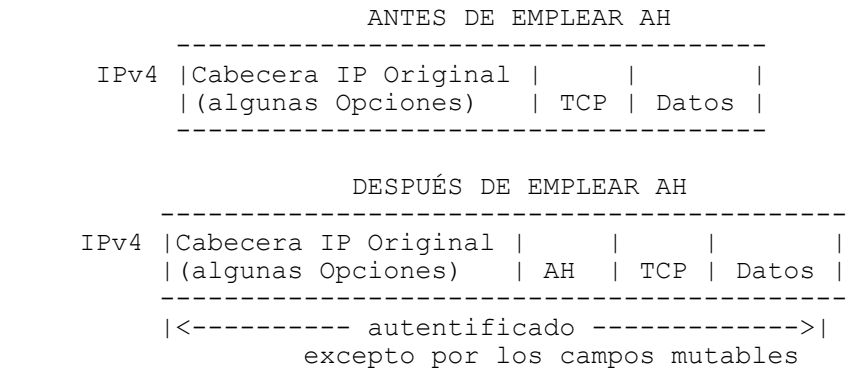
Este campo es de longitud variable y contiene el Valor de Comprobación de Integridad (ICV) para este paquete. Este campo debe contener un múltiplo entero de 32 bits de longitud. Los detalles del cálculo de ICV se describen en la Sección 3.3.2. Este campo puede incluir relleno explícito (apreciable). Este relleno se incluye para asegurarse de que la longitud de la cabecera de AH sea múltiplo entero de 32 bits (en IPv4) o de 64 bits (en IPv6). Todas las implementaciones DEBEN soportar tales rellenos. Los detalles de cómo calcular la longitud del relleno se proporcionan abajo. El algoritmo de autentificación DEBE especificar la longitud ICV y las reglas de comparación y los pasos de procesamiento para la validación.

3. Procesamiento de la Cabecera de Autentificación

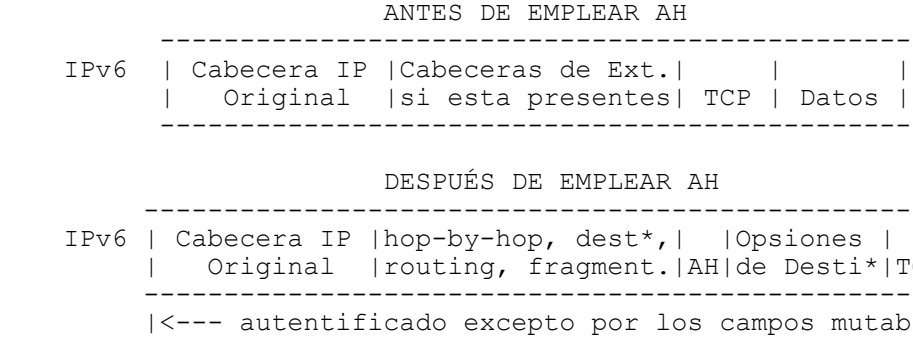
3.1 Localización de la Cabecera de Autentificación

Al igual que ESP, HA se puede emplear de dos modos: modo trasporte o modo túnel. El modo trasporte es aplicable solamente a implementaciones host y proporciona protección para los protocolos de capa superiores, además de los campos seleccionados de la cabecera IP. (En este modo, observe que para las implementaciones "Puesto-en-la-Pila" (BITS: Bump-in-the-snack) o "Puesto-en-el-cable" (BITW: bump-in-the-wire), según lo definido en el documento Arquitectura de Seguridad, fragmentos IP entrantes y salientes se pueden precisar en una implementación IPsec para realizar el reensamblaje/fragmentación IP conforme a esta especificación y proporcionar soporte IPsec transparente. Cuidado especial se requiere para realizar tales operaciones dentro de estas implementaciones cuando múltiples interfaces están funcionando.)

En modo trasporte, AH se inserta después de la cabecera IP y antes del protocolo de capa superior, por ejemplo, TCP, UDP, ICMP, etc. o antes de cualquier otra cabecera IPsec que ya se haya incluido. En el contexto de IPv4, esto requiere colocar AH después de la cabecera IP (y de cualquier opción que esta contenga), pero antes del protocolo de capa superior. (Observe que el término modo "transporte" no debería ser mal interpretado restringiendo su uso a TCP y a UDP. Por ejemplo, un mensaje ICMP se PUEDE enviar usando modo "transporte" o modo "túnel".) El diagrama siguiente ilustra a AH en modo trasporte para un paquete típico IPv4, "antes y después" de haberle aplicado AH en modo trasporte.



En el contexto IPv6, el AH se ve como carga extremo-a-extremo (end-to-end), y debe aparecer después de las cabeceras de extensión: salto-por-salto (hop-by-hop), de encaminamiento (routing), y de fragmentación. Las cabecera(s) de extensión opciones de destino podrían aparecer antes o después de la cabecera AH dependiendo de la semántica deseada. El diagrama siguiente ilustra AH en modo trasporte colocado en un paquete típico de IPv6.

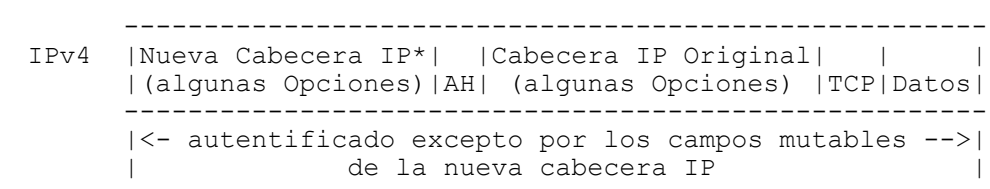


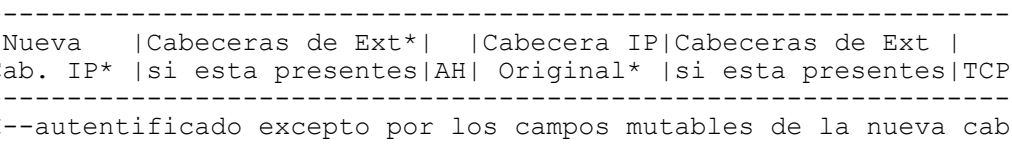
* = si están presentes, pueden estar antes que AH, después de AH, o en ambos.

Las cabeceras ESP y AH se pueden combinar de varias formas. El documento de la Arquitectura IPsec describe las combinaciones de Asociaciones de Seguridad que deben ser soportadas.

AH en modo túnel puede ser empleado en host o securitys gateway (o en implementaciones llamadas "Puesto-en-la-Pila" (BITS) o "Puesto-en-el-cable" (BITW), según lo definido en el documento de la Arquitectura de seguridad). Cuando AH se implementa en una security gateway

(protege tráfico en tránsito), el modo túnel debe ser utilizado. En modo túnel, la cabecera IP "interna" lleva la última dirección de origen y de destino, mientras que la cabecera IP "externa" puede contener distintas direcciones IP, por ejemplo, direcciones de securitys gateway. En modo túnel, AH protege el paquete IP interno completamente, incluyendo la cabecera IP interna entera. La posición de AH en modo túnel, concerniente a la cabecera IP exterior, es igual que para AH en modo trasporte. El diagrama siguiente ilustra AH en modo túnel que se coloca para los paquetes típicos IPv4 y IPv6.





* = Construcción de otras cabeceras IP y/o de extensión y modificación de la cabecera IP interna y/0 de extensión según lo debatido mas abajo.

3.2 Algoritmos de Autentificación

El algoritmo de autentificación empleado para el cálculo de ICV esta especificado por la SA. Para las 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 comunicaciones 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. Los algoritmos de autentificación que deben implementarse obligatoriamente se describen en la Sección 5 "Requerimientos de Conformidad". Otros algoritmos PUEDEN ser empleados.

3.3 Procesamiento de Paquetes Salientes

En modo trasporte, el emisor inserta la cabecera AH después de la cabecera IP y antes de la cabecera del protocolo de capa superior, como se describió anteriormente. En modo túnel, la cabeceras externas y internas IP/de extensiones se pueden interrelacionar de varias formas. La construcción de las cabeceras externas IP/extensiones llevadas a cabo durante el proceso de encapsulación se describen en el documento de la Arquitectura de Seguridad.

Si se requiere más de una cabecera IPsec/extensión, el orden de aplicación de las cabeceras de seguridad DEBE estar definido por la política de seguridad. Para la simplicidad del procesamiento, cada cabecera de IPsec DEBERÍA ignorar la existencia (es decir, no fijar a cero los contenidos o no intentar predecir los contenidos) de las cabeceras de IPsec que se aplicarán después. (Mientras que una implementación IP nativa o BITS podría predecir los contenidos de las últimas cabeceras IPsec a las que esta implementación se aplicó, no será posible que esta implementación prediga ninguna de las cabeceras IPsec agregadas por una implementación BITW entre el host y la red.)

3.3.1 Búsqueda de Asociaciones de Seguridad

AH se aplica a un paquete saliente solamente después de que una implementación IPsec determine que el paquete está asociado con una SA la cual requiere el procesamiento de AH. 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 Generación del Número de Secuencia

El contador del emisor es inicializado a 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 nuevamente a cero.

3.3.3 Cálculo del Valor de Comprobación de Integridad

El ICV de AH es calculado sobre:

- Los campos de la cabecera IP que son inmutables en tránsito o que son predecibles en valor al momento de la llegada en los extremos para la SA AH.
- La cabecera de AH (Cabecera Siguiente, Longitud de la Carga, Reservado, SPI, Número de Secuencia, y los Datos de Autentificación (se fijan a cero para este cálculo), y los bytes explícitos de relleno (si los hay)).
- Los datos del protocolo de nivel superior, que se asumen son inmutables en tránsito.

3.3.3.1 Manipulación de los Campos Mutables

Si un campo puede ser modificado durante el tránsito, el valor del campo se fija a cero para los propósitos del cálculo del ICV. Si un campo es mutable, pero su valor en el receptor (IPsec) es predecible, entonces ese valor es insertado en el campo para los propósitos del cálculo del ICV. El campo Datos de Autentificación también se fija a cero en preparación para este cálculo. Observe que reemplazando el valor de cada campo por cero, en lugar de omitir el campo, la alineación es preservada para el cálculo del ICV. También, el método de colocar el valor cero asegura que la longitud de los campos que son manipulados no se pueda cambiar durante el tránsito, aun cuando sus contenidos no son cubiertos explícitamente por el ICV.

Si se crea una nueva cabecera de extensión o de opción en IPv4, esta será definida en su propio RFC y DEBERÍA incluir (en la sección de Consideraciones de Seguridad) la forma de cómo se debería manipular el cálculo del ICV de AH. Si la implementación IP (IPv4 o IPv6) encuentra una cabecera de extensión que no reconoce, desechará el paquete y enviará un mensaje ICMP. IPsec nunca verá el paquete. Si la implementación IPsec encuentra una opción IPv4 que no reconoce,

debería poner a cero la opción entera, usando el segundo byte de la opción como la longitud. Las opciones de IPv6 (en las cabeceras de extensión de Destino o la de Salto por Salto) contienen una bandera que indica la mutabilidad, que determina el procesamiento apropiado para tales opciones.

3.3.3.1.1 Cálculo de ICV para IPv4

3.3.3.1.1.1 Campos de la Cabecera Base

Los campos de la cabecera base de IPv4 se clasifican de la siguiente manera:

Inmutables
- Versión
- Longitud de la Cabecera Internet
- Longitud Total
- Identificación
- Protocolo (éste debería tener el valor para AH.)
- Dirección de Origen
- Dirección de Destino (sin una ruta de destino estricta o libre)

Mutable pero predecible
- Dirección de Destino (con ruta de destino estricta o libre)

Mutable (se colocan a cero antes del cálculo del ICV)
- Tipo de Servicio (TOS)
- Banderas (Flags)
- Desplazamiento del Fragmento
- Tiempo de Vida (TTL)
- Suma de Verificación de la Cabecera

TOS -- Este campo es excluido porque se sabe que algunos routers cambian el valor de este campo, aunque la especificación de IP no considera al TOS como un campo mutable de la cabecera.

Banderas -- Este campo es excluido puesto que routers intermedios puede fijar el bit de DF, incluso si el origen no lo seleccionó.

Desplazamiento del Fragmento -- Puesto que AH se aplica solamente a paquetes IP no a fragmentados, el Campo Desplazamiento debe ser siempre cero, y así excluido (aunque es predecible).

TTL -- Éste es cambiado en ruta como curso normal del procesamiento por routers, y así su valor en el receptor no es predecible por el emisor.

Suma de Verificación de la Cabecera -- Esta cambiará si alguno de estos otros campos cambian, y así su valor en la recepción no se puede predecir por el emisor.

3.3.3.1.1.2 Opciones

Para IPv4 (no así para IPv6), no hay mecanismos para marcar opciones como mutables en tránsito. Por lo tanto las opciones IPv4 se en listan explícitamente en el Apéndice A y se clasifican como: inmutables, mutable pero predecible, o mutables. Para IPv4, la opción entera se ve como una unidad; por lo tanto el tipo y longitud de los campos dentro de la mayoría de las opciones son inmutables en tránsito, si una opción se clasifica como mutable, la opción entera se pone en cero para los propósitos del cálculo del ICV.

3.3.3.1.2 Cálculo de ICV para IPv6

3.3.3.1.2.1 Campos de la Cabecera Base

Los campos de la cabecera base IPv6 se clasifican de la siguiente manera:

Inmutable
- Versión
- Longitud de la Carga
- Cabecera Siguiente (ésta debería tener el valor para AH.)
- Dirección de Origen
- Dirección de Destino (sin la Cabecera de Extensión de Ruteo)

Mutable pero predecible
- Dirección de Destino (con la Cabecera de Extensión de Ruteo)

Mutable (puesto a cero para el cálculo de ICV)
- Clase
- Etiqueta de Flujo
- Límite de Saltos

3.3.3.1.2.2 Cabeceras de Extensión que Contienen Opciones

Las opciones IPv6 de las Cabeceras de Extensión de, Salto por Salto y de Destino contienen un bit que indican si la opción puede o no cambiar (de forma impredecible) durante el tránsito. Para cualquier

opción para la cual los contenidos puedan cambiar en tránsito, todo el campo "Datos Opcionales" debe ser tratado con valor de cero octetos al calcular o verificar del ICV. El Tipo de Opción y la Longitud de los Datos Opcionales se incluyen en el cálculo del ICV. Todas las opciones para las cuales el bit indica inmutabilidad se incluyen en el cálculo del ICV. Vea la especificación de IPv6 [DH95] para más información.

3.3.3.1.2.3 Cabeceras de Extensión que no Incluyen Opciones

Las cabeceras de extensión de IPv6 que no contienen opciones se incluyen explícitamente en el Apéndice A y se clasifican como: inmutables, mutable pero predecibles, o mutables.

3.3.3.2 Relleno

3.3.3.2.1 Relleno de los Datos de Autentificación

Según lo mencionado en la sección 2.6, el campo Datos de Autentificación incluye explícitamente el relleno para asegurarse de que la cabecera de AH es un múltiplo de 32 bits (para IPv4) o de 64 bits (para IPv6). Si se requiere el relleno, su longitud es determinada por dos factores:

- la longitud del ICV
- la versión del protocolo IP (IPv4 o IPv6)

Por ejemplo, si la salida del algoritmo seleccionado es de 96 bits, no se requerirá ningún relleno para IPv4 o para IPv6. Sin embargo, si se genera una longitud ICV distinta, debido al uso de un algoritmo diferente, entonces el relleno puede ser requerido dependiendo de la longitud y de la versión del protocolo IP. El contenido del campo de relleno es seleccionado arbitrariamente por el emisor. (El relleno es arbitrario, pero necesita no ser aleatorio para lograr seguridad.) Estos bytes de relleno se incluyen en el cálculo de los Datos de Autentificación, se cuentan como parte de la Longitud de la Carga y se transmiten al final del campo Datos de Autentificación para permitir al receptor realizar el cálculo del ICV.

3.3.3.2.2 Relleno Implícito del Paquete

Para algunos algoritmos de autentificación, la cadena de bytes sobre la cual el cálculo del ICV se realiza debe ser un múltiplo de un tamaño de bloque especificado por el algoritmo. Si la longitud del paquete IP (incluido AH) no coincide con los requisitos del tamaño de bloque para el algoritmo, el relleno implícito DEBE ser aplicado al

final del paquete, 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 por la especificación del algoritmo. Este relleno no se transmite con el paquete. Observe que MD5 y SHA-1 tienen un tamaño de bloque de un byte debido a sus convenciones internas del relleno.

3.3.4 Fragmentación

Si se requiere, la fragmentación IP ocurre después del procesamiento de AH dentro de una implementación IPsec. Así, en modo trasporte AH se aplica solamente a los datagramas IP enteros (no a los fragmentos IP). Un paquete IP al cual se ha aplicado AH se puede fragmentar por routers en ruta, y tales fragmentos se deben reensamblar antes de que AH sea procesado por el receptor. En modo túnel, AH se aplica a un paquete IP, el cual la carga puede ser un paquete IP fragmentado. Por ejemplo, en una security gateway o en implementaciones IPsec BITS o BITW (véase el documento de Arquitectura de Seguridad para más detalles) se puede aplicar AH en modo túnel a tales fragmentos.

3.4 Procesamiento de Paquetes Entrantes

Si hay más de una cabecera/extensión de IPsec presente, el procesamiento para cada una ignorará (no pone a cero, no usa) cualquier cabecera IPsec subsiguiente aplicada a la cabecera que esta siendo procesada.

3.4.1 Reensamblaje

Si se requiere, el reensamblaje se realiza antes del procesamiento de AH. Si un paquete brindado a AH 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, 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 que contiene una Cabecera de Autentificación, el receptor determina la SA (unidireccional) apropiada, basándose en la Dirección de Destino IP, el Protocolo de Seguridad (AH), 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, especifica el/los algoritmo/s empleados para el cálculo del ICV, y indica la/s clave/s requerida/s para validar el ICV.

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, y (en IPv6) el Identificador de Flujo (Flow ID).

3.4.3 Verificación del Número de Secuencia

Todas las implementaciones de AH DEBEN soportar el servicio de anti-replay, aunque su uso puede estar habilitado o deshabilitado por el receptor sobre la base de una SA. (Observe que no hay provisiones para administrar los valores de los Números 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-emisor que emplee una única SA.)

Si el receptor no habilita el anti-replay para una SA, no se realizará las comprobaciones entrantes 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 3.3.2), 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 AH 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 ventana.

El lado "Derecho" de la ventana representa el valor del 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 del Número de Secuencia.

3.4.4 Verificación del Valor de Comprobación de Integridad

El receptor calcula el ICV sobre los campos apropiados del paquete, usando el algoritmo de autentificación especificado, y verifica que es el mismo que el ICV incluido en el campo Datos de Autentificación de el 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.

DISCUSIÓN:

Comience guardando el valor ICV y reemplácelo con cero (pero no por un relleno de Datos de Autentificación). Ponga a cero el resto de los campos que han sido modificados durante el tránsito. (Ver la Sección 3.3.3.1 para una discusión sobre que campos son puestos a cero antes de realizar el cálculo del ICV.) Controle la longitud total del paquete, y si se requiere relleno implícito basado en los requerimientos del algoritmo de autentificación, se agregan los bytes de relleno con valor cero en el extremo del paquete como es requerido. Realice el cálculo del ICV y compare el resultado con el valor guardado, usando las reglas de comparación definidas por la especificación 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.)

4. Auditoría

No todos los sistemas que implementan AH implementarán auditoría. Sin embargo, si AH es incorporado a un sistema que soporta auditoría, la implementación AH debe también soportar auditoría y debe permitirle a un administrador de sistema habilitar o deshabilitar la auditoría para AH. 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 AH, los procesos descriptos aquí y 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 manuales. Una implementación AH debe soportar e implementar obligatoriamente los siguientes algoritmos:

- HMAC con MD5 [MG97a]
- HMAC con SHA-1 [MG97b]

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 1826

Este documento se diferencia del RFC 1826 [ATK95] en varias formas significativas, las características fundamentales de AH quedan intactas. Un propósito de la revisión del RFC 1826 fue proporcionar un marco completo para AH con RFCs auxiliares requeridos solamente para la especificación del algoritmo. Por ejemplo el servicio de anti-replay es ahora una parte integral y obligatoria de AH, y no una característica de una transformación definida en otro RFC. El trasporte del número de secuencia para soportar este servicio ahora se requiere siempre. El algoritmo por defecto requerido para la interoperatibilidad ha sido cambiado a HMAC con MD5 o SHA-1 (vs. claves MD5), por razones de seguridad. La lista de campos de cabecera IPv4 excluidas del computo ICV han sido expandidas para incluir los campos desplazamiento (OFFSET) y banderas (FLAGS).
Otra motivación para la revisión fue proporcionar detalles adicionales y la planificación de puntos sutiles. Esta especificación proporciona fundamento para la exclusión de campos de cabecera IPv4 seleccionados de AH y proporciona ejemplos de la colocación de AH en contextos IPv4 y IPv6. Los requerimientos de auditoría ha sido clarificados en la versión de la especificación. En modo túnel AH fue mencionado solamente al pasar del RFC 1826, pero ahora es una característica obligatoria de AH. La discusión de interacciones con administración de claves y con las etiquetas de seguridad ha sido movida al documento de la Arquitectura de seguridad.

Agradecimientos

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 significativas 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 y 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, Francis Dupont, Phil Karn, Frank Kastenholz, Perry Metzger, David Mihelcic, Hilarie Orman, Norman Shulman, William Simpson, and Nina Yuan.

Apéndice A -- Mutabilidad de Opciones IP/Cabeceras de Extensión

A1. IPv4 Opciones

Esta tabla muestra como las opciones de IPv4 están clasificadas de acuerdo a la "mutabilidad". Donde dos referencias son proporcionadas, la segunda sustituye a la primera. Esta tabla está basada en la información proporcionada en el RFC 1700, NÚMEROS ASIGNADOS, (octubre 1994).

Copy	Class	Opt. #	Nombre	Referencia
INMUTABLE	------	Incluidos en el cálculo de ICV		
0	0	0	Final de la lista de opciones	[RFC791]
0	0	1	No operación	[RFC791]
1	0	2	Seguridad	[RFC1108(histórico pero en uso)]
1	0	5	Extensión de seguridad	[RFC1108(histórico pero en uso]
1	0	6	Seguridad comercial	[expiro I-D, ahora uso US MIL STD]
1	0	20	Alerta de Router	[RFC2113]
1	0	21	dirección del emisor de entrega multi-destino	[RFC1770]
MUTABLE	---------	poner en cero		
1	0	3	Ruta de origen no fija	[RFC791]
0	2	4	Fecha de registro	[RFC791]
0	0	7	Registrar ruta	[RFC791]
1	0	9	Ruta de origen estricta	[RFC791]
0	2	18	Traceroute	[RFC1393]
Experimental, SUSTITUIR	----	poner en cero		
1	0	8	Identificador de Flujo	[RFC791, RFC1122 (Host Req)]
0	0	11	Prueba de MTU	[RFC1063, RFC1191 (PMTU)]
0	0	12	MTU Reply	[RFC1063, RFC1191 (PMTU)]
1	0	17	Extended Internet Proto	[RFC1063, RFC1191 (PMTU)]
0	0	10	Medición experimental	[ZSu]
1	2	13	Control de Flujo experimental	[Finn]
1	0	14	Control de Acceso Experimental	[Estrin]
0	0	15	???	[VerSteeg]
1	0	16	Descriptor de trafico IMI	[Lee]
1	0	19	Extensión de direcciones	[Ullmann IPv7]

Nota: El uso de la opción de alerta de router es incompatible con el uso de IPsec. Aunque la opción es inmutable, su uso implica que cada router a través de la trayectoria del paquete "procesará" el paquete y consecuentemente podría cambiar el paquete, esto podría pasar, en las bases de un salto por salto a medida de que el paquete vaya de router a router. Antes de ser procesado por la aplicación por la cual los contenidos están controlados, por ejemplo, RSVP/IGMP, el paquete debería ser procesado por AH.

Sin embargo el procesamiento de AH, requerirá que cada router a través de la trayectoria sea miembro de una SA multicast definida por el SPI. Esto puede plantear problemas para los paquetes que no están encaminados a un origen estricto, y requiere que las técnicas de soporte multicast no estén disponibles.

NOTA: el agregado o el removido de cualquier etiqueta de seguridad (BSO, ESO, CIPSO), por sistemas a través de la trayectoria de un paquete esta en conflicto con la clasificación de inmutables de estas Opciones IP y es incompatible con el uso de IPsec.

NOTA: Las opciones Final de la Lista de Opciones DEBERÍA ser repetida como sea necesario para asegurar que la cabecera IP termina en un limite de 4 bytes para asegurar que no hay bytes no especificados que se podrían utilizar para un canal secreto.

A2. Cabeceras de Extensión de IPv6

Esta tabla muestra como las Cabeceras de Extensión de IPv6 están clasificadas de acuerdo a la "mutabilidad".

Opción/Extensión Nombre	Referencia
Mutable pero predecible --- Incluidos en el cálculo de ICV	
Ruteo (Tipo 0)	[RFC1883]
EL BIT INDICA SI LA OPCIÓN ES MUTABLE (CAMBIA EN FORMA IMPREDECIBLE DURANTE EL TRÁNSITO	
Opciones Salto por Salto	[RFC1883]
Opciones de Destino	[RFC1883]
No Aplicable	
Fragmentación	[RFC1883]

Opciones -- Las cabeceras de opción de Salto por Salto y de Destino de IPv6 contienen un bit que indican si la opción puede cambiar impredeciblemente durante el tránsito. Para cada opción cuyo contenido puede cambiar en ruta, el campo entero "Datos de Opción" debe ser tratado como octetos con

valor cero al momento del cálculo o verificación del ICV. El campo Tipo de Opción y la Longitud de los Datos de la Opción están incluidos en el cálculo del ICV. Todas las opciones cuyos bits indiquen inmutabilidad están incluidas en el cálculo del ICV. Ver la especificación de IPv6 [DH95] para más información.

Ruteo (Tipo 0) -- La Cabecera de Ruteo de IPv6 "Tipo 0" cambiará solo los campos de dirección dentro del paquete durante el tránsito del origen al destino. Sin embargo, los contenidos del paquete como aparecerán en el receptor y todos los saltos intermedios, son conocidos por el emisor. Por lo tanto, la Cabecera de Ruteo de IPv6 "Tipo 0" esta incluida en el cálculo de los Datos de Autentificación como mutable pero predecible. El emisor debe ordenar el campo de tal forma de que aparezca como se verá en el receptor, antes de realizar el cálculo del ICV.

Fragmentación -- Ocurre después del procesamiento IPsec saliente (Sección 3.3) y el reensamblaje ocurre antes del procesamiento IPsec de entrada (Sección 3.4). Por lo tanto la Cabecera de Extensión de Fragmentación, si existe, no es vista por IPsec.

Observe que en el lado del receptor, la implementación IP podría dejar una Cabecera de Extensión de Fragmentación en su sitio al momento de hacer el reensamblaje. Si esto pasa, cuando AH recibe el paquete, antes de realizar el proceso ICV, AH debe "quitar" (o saltarla) esta cabecera y cambiar la cabecera anterior del campo "Cabecera Siguiente" para que sea el campo "cabecera siguiente" en la Cabecera de Extensión de Fragmentación.

Observe que en el lado del emisor, la implementación IP podría dar al código IPsec un paquete con una Cabecera de Extensión de Fragmentación con un Desplazamiento de cero (primer fragmento) y una Bandera de Más Fragmentos de cero (ultimo fragmento). Si esto pasa, antes de hacer el proceso ICV, AH primero debe "quitar" (o saltar sobre) esta cabecera y cambiar la cabecera anterior del campo "Cabecera Siguiente" para que sea el campo "cabecera siguiente" en la Cabecera de Extensión de Fragmentación.

Referencias

[ATK95] Atkinson, R., "The IP Authentication Header", RFC 1826, August 1995.

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

[DH95] Deering, S., and B. Hinden, "Internet Protocol version 6 (IPv6) Specification", RFC 1883, December 1995.

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

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

[KA97b] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

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

Notas del Traductor

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. Declaración Completa de Copyright

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

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