Grupo de Trabajo en Red
Request for Comments: 2403
Categoría: Pila de Estándares

C. Madson
Cisco Systems Inc.
R. Glenn
NIST

Noviembre 1998

Traducción al castellano:
Hugo Adrian Francisconi <adrianfrancisconi@yahoo.com.ar>

Agosto 2005

Uso de HMAC-MD5-96 en ESP y AH

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

Resumen

Este documento describe el uso del algoritmo HAMC [RCF-2104] en conjunto con el algoritmo MD5 [RFC-1321] como mecanismo de autentificación, para la Carga de Seguridad Encapsulada [ESP] y para la Cabecera de Autentificación [AH] dentro de IPsec. HMAC con MD5 proporcionan autentificación del origen de datos y protección de integridad.

Información adicional sobre otros componentes necesarios para implementaciones de ESP y AH es proporcionada por [Thayer97a].

1. Introducción

Este documento especifica el uso de MD5 [RFC-1321] combinado con HMAC [RFC-2104], como un mecanismo de autentificación de claves dentro del contexto de ESP y AH dentro de IPsec. El propósito de HMAC-MD5-96 es asegurar que el paquete es autentico y que no puede ser modificado en tránsito.

HMAC es un algoritmo de autentificación de clave secreta. La integridad de los datos y la autentificación del origen de los datos como es proporcionada por HMAC es dependiente del alcance de la distribución de la clave secreta. Si solamente el origen y el destino conocen la clave HMAC, esto proporciona autentificación del origen de los datos e integridad de los datos para los paquetes enviados entre las partes; si el HMAC es correcto, esto prueba que el HMAC a sido agregado por el origen.

En este documento, HMAC-MD5-96 es usado dentro del contexto de ESP y AH. Para más información de como varias partes de ESP (incluyendo mecanismos de confidencialidad) se unen para proporcionar servicios de seguridad, referirse a [ESP] y a [Thayer97a]. Para más información sobre AH, referirse a [AH] y a [Thayer97a].

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].

2. Algoritmo y Modo

El [RFC-1321] describe el algoritmo fundamental MD5, mientras que el [RFC-2104] describe el algoritmo HMAC. El algoritmo HMAC proporciona un marco para insertar varios algoritmos de hash como el MD5.

HMAC-MD5-96 opera sobre bloques de datos de 64 bits. Los requerimientos para el relleno están especificados en [RFC-1321] y son parte del algoritmo MD5. Si usted construye el MD5 de acuerdo con [RFC-1321] no necesitará agregar rellenos adicionales para HMAC-MD5-96. Con respecto al "relleno del paquete implícito" como lo define [AH] no es requerido.

HMAC-MD5-96 produce un valor de autentificación de 128 bits. Este valor de 128 bits puede ser acortado como se describe en el RFC 2104. Para usarse con ESP o AH, un valor truncado usando los primeros 96 bits BEBE ser soportado. En el envío, el valor truncado es almacenado dentro del campo de autentificación. En la recepción el valor completo de 128 bits es calculado y los primeros 96 bits son comparados con el valor almacenado en el campo autentificación. Ninguna otra longitud del valor de autentificación es soportado por HMAC-MD5-96.

La longitud de 96 bits fue seleccionada porque es la longitud de autentificación por defecto como está especificado en [AH] y soluciona los requisitos de seguridad descriptos en [RFC-2104].

2.1 Funcionamiento

[Bellare96a] indica que "el funcionamiento (de HMAC) es esencialmente el de la función hash principal". El [RFC-1810] proporciona análisis del funcionamiento y recomendaciones del uso de MD5 con protocolos de Internet. Al momento de realizar este documento no se había realizado análisis del funcionamiento de HMAC o HMAC combinado con MD5.

El [RFC-2104] describe una modificación de implementación que puede mejorar el funcionamiento por paquete sin afectar a la interoperatibilidad.

3. Material Clave

HMAC-MD5-96 es un algoritmo de clave secreta. A pesar de que ninguna longitud de clave fija es especificada en [RFC-2104], cuando se usa en ESP o AH una longitud de clave fija de 128 bits DEBE ser soportada. Longitudes de claves distintas de 128 bits no DEBEN ser soportadas (es decir solamente claves de 128 bits deben ser usadas por HMAC-MD5-96). Una longitud de clave de 128 bits fue elegida basándose en las recomendaciones del [RFC-2104] (es decir longitudes de claves menores a la longitud de autentificación debilitan la seguridad y claves más largas que la longitud de autentificación no incrementan la seguridad).

El [RFC-2104] discute los requerimientos sobre el material clave, incluyendo una discusión de requerimientos de aleatoriedad fuerte. Una función seudo-aleatoria fuerte DEBE ser usada para generar la clave de 128 bits requerida.

Al momento en que se produjo este documento no hay claves débiles especificadas para el uso de HMAC. Esto no significa que no existan. Si, en algún momento, un conjunto de claves débiles para HMAC es identificado, el uso de estas claves débiles debe ser rechazado, seguido de una solicitud de reemplazo de claves o una negociación de nueva SA.

Para proporcionar la autentificación del origen de los datos, los mecanismos de distribución de claves deben asegurar que claves únicas sean asignadas y que estén distribuidas solamente a las partes participantes en la comunicación.

El [RFC-2104] hace la siguiente recomendación con relación al recambio de claves. Los ataques actuales no indican una frecuencia específica para el cambio de claves ya que estos ataques son prácticamente impracticables. Sin embargo, la renovación periódica de

las claves es una práctica de seguridad fundamental que ayuda contra debilidades potenciales de la función y claves, reduce la información disponible a un criptoanálisis y limita el daño de una clave expuesta.

4. Interacción con los mecanismos de cifrado de ESP

Al momento de la creación de este documento no hay teman conocidos que excluyan el uso del algoritmo HMAC-MD5-96 con ningún algoritmo especifico de cifrado.

5. Consideraciones de seguridad

La seguridad proporcionada por HMAC-MD5-96 se basa en la fuerza de HMAC, y en menor grado, en la fuerza de MD5. El [RFC-2104] requiere que HMAC no dependa de la propiedad de la resistencia fuerte a colisiones, que es importante de considerar cuándo se evalúa el uso de MD5, aunque, bajo pruebas recientes, a mostrado ser menos resistente a colisiones que en un primer momento. Al momento de la creación de este documento no hay ataques criptográficos prácticos contra HMAC-MD5-96.

El [RFC-2104] indica que para que las "funciones hash sean minímamente coherentes" el birthday attack, el ataque más fuerte conocido contra HMAC, sea impracticable. Para un bloque de hash de 64 bits tal como HMAC-MD5-96 un ataque incluyendo el procesamiento exitoso de bloques de 2^64 no sería práctico a menos que se hubiera descubierto que el hash principal tuvo colisiones después de procesar bloques de 2^30 Un hash con tales características de resistencia débil a colisiones sería generalmente considerado inservible.

También es importante considerar que mientras que MD5 nunca fue desarrollado para ser usado como un algoritmo de clave hash, HMAC tuvo ese criterio desde el principio. Mientras que el uso de MD5 en el contexto de seguridad de datos esta experimentando la reevaluación, la combinación de HMAC con el algoritmo MD5 ha estado sujeto a examen criptográfico.

El [RFC2104] también habla de la seguridad adicional potencial que es proporcionada por el acortamiento del hash resultante. Las especificaciones que incluyen HMAC están fuertemente impulsadas a realizar este acortamiento de hash.

Como el [RFC-2104] proporciona un marco para incorporar varios algoritmos de hash con HMAC, es posible reemplazar MD5 con otros algoritmos tales como SHA-1. El [RFC-2104] contiene una detallada discusión sobre las fortalezas y debilidades de algoritmos HMAC.

Así como es cierto que para cualquier algoritmo criptográfico, parte de su fuerza recae en la correcta aplicación del algoritmo, la seguridad del mecanismo de administración de clave y su implementación, la fuerza de la clave secreta asociada y sobre la correcta implementación de todos los sistemas participantes. El [RFC-2202] contiene vectores de prueba y ejemplos de código para asistir en la verificación de la exactitud del código HMAC-MD5-96.

6. Agradecimientos

Este documento deriva en parte de trabajos previos realizados por Jim Hughes, aquella gente que trabajó con Jim Hughes en la transformaciones combinadas DES/CBC+HMAC-MD5 ESP, la ANX participantes bakeoff, y los miembros del grupo de trabajo de IPsec.

También nos gustaría agradecer a Hugo Krawczyk por sus comentarios y recomendaciones acerca de ciertos textos criptográficos específicos en este documento.

7. Referencias

[RFC-1321] Rivest, R., "MD5 Digest Algorithm", RFC 1321, April 1992.

[RFC-2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC-1810] Touch, J., "Report on MD5 Performance", RFC 1810, June 1995.

[Bellare96a] Bellare, M., Canetti, R., and H. Krawczyk, "Keying Hash Functions for Message Authentication", Advances in Cryptography, Crypto96 Proceeding, June 1996.

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

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

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

[Thayer97a] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[RFC-2202] Cheng, P., and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1", RFC 2202, March 1997.

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

8. Direcciones de los Autores

Cheryl Madson
Cisco Systems, Inc.
EMail: cmadson@cisco.com

Rob Glenn
NIST
EMail: rob.glenn@nist.gov

The IPsec working group can be contacted through the chairs:

Robert Moskowitz
ICSA
EMail: rgm@icsa.net

Ted T'so
Massachusetts Institute of Technology
EMail: tytso@mit.edu

9. Declaración de Copyright Completa

Notas del Traductor

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

. birthday attack (ataque del día de cumpleaños): El nombre deriva de la probabilidad de que dos o más personas en un grupo de 23 personas, compartan la misma fecha de cumpleaños es menor que 0.5, (conocida como paradoja del cumpleaños). El birthday attack es un nombre usado para referirse a una clase de ataque por fuerza bruta. Para una función hash que tiene como salida una cadena de 160 bits, es necesario recorrer entonces 2^80 mensajes para poder encontrar dos con el mismo hash, o sea encontrar una colisión.

Los Términos que aparecen entre "[]" que no sean referencias reflejan la palabra/s en ingles 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 termino o simplemente para que no se pierda el VERDADERO sentido del texto.

La referencia [DOI] descripta en este RFC (RFC 2410) hace referencia al RFC 2408 (ISAKMP) pero me parece que los autores realmente quisieron hacer referencia al RCF 2407 (IP Security Domain of Interpretation).

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