Grupo de Trabajo en Red
Request for Comments: 2405
Categoría: Pila de Estándares

C. Madson
Cisco Systems Inc.
N. Doraswamy
Bay Networks, Inc.

Noviembre 1998

Traducción al castellano:
Agosto 2005

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

El Algoritmo de Cifrado DES-CBC en ESP con IV explicito

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 de cifrado DES en Modo Encadenamiento de Bloque Cifrado (CBC), con un Vector de Inicialización (IV) explícito, como mecanismo de confidencialidad dentro del contexto de la Carga de Seguridad Encapsulada (ESP) en IPsec.

1. Introducción

Este documento describe el uso del algoritmo de cifrado DES en Modo Encadenamiento de Bloque Cifrado (CBC) como mecanismo de confidencialidad dentro del contexto ESP, de ahora en adelante denominado DES-CBC en ESP o simplemente DES-CBC.

El DES es un algoritmo de cifrado de bloque simétrico. El algoritmo se describe en [FIPS-46-2] [FIPS-74] [FIPS-81]. [Schneier96] proporciona una descripción general del Modo Encadenamiento de Bloque Cifrado, un modo que es aplicable a varios algoritmos de encriptación.

Según lo especificado en esta nota, DES-CBC no es un mecanismo de autentificación. (Aunque DES-MAC, descrito en [Schneier96] entre otros lugares, proporciona autentificación, DES-MAC no se discute aquí.)

Para más información sobre cómo diversas partes de ESP se juntan para proporcionar servicios de seguridad, referirse a [ESP] y [Road].

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 [RFC-2119].

2. Algoritmo y Modo

DES-CBC es un algoritmo de bloque de clave secreta simétrica. Tiene un tamaño de bloque de 64 bits.

[FIPS-46-2] [FIPS-74] y [FIPS-81] describen el algoritmo DES, mientras que [Schneier96] proporciona una buena descripción del modo CBC.

2.1 Funcionamiento

Phil Karn ha perfeccionado software DES-CBC para alcanzar velocidades de hasta 10.45 Mbps con una Pentium 90 MHz., ascendiendo a 15.9 Mbps con una Pentium 133 MHz. Otras velocidades estimadas de DES pueden ser encontradas en [Schneier96].

3. Carga ESP

DES-CBC requiere de un Vector de Inicialización (IV) explícito de 8 octetos (64 bits). Este IV precede a la carga protegida (encriptada). El IV DEBE ser un valor aleatorio.

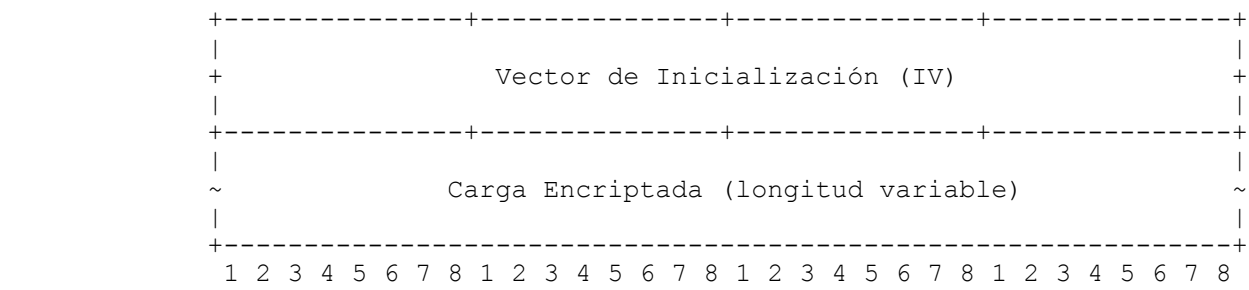
Incluir el IV en cada datagrama asegura de que la desencriptación de cada datagrama recibido pueda ser realizada, incluso cuando algunos datagramas se pierden, o lleguen en desorden.

Nota de implementación:

La práctica común es utilizar datos aleatorios para el primer IV y los últimos 8 octetos de datos encriptados de un proceso de encriptación se usan para el IV del siguiente proceso de encriptación; esto extiende la lógicamente CBC a través de los paquetes. También tiene la ventaja de limitar la filtración de información del número generado aleatoriamente. No importa qué

mecanismos se utilicen, el receptor NO DEBE asumir ningún significado de este valor, con excepción de que ése es un IV.
Para evitar encriptación ECB de bloques de texto plano de la misma manera en diferentes paquetes, las implementaciones NO DEBEN utilizar un contador o otro origen de distancia de Hamming bajo (Ver "distancia de Hamming" en Notas del Traductor) para IVs.

El campo carga, según lo definido en [ESP], se analiza según el siguiente diagrama:



3.1 Tamaño del Bloque y Relleno

El algoritmo DES-CBC descripto en este documento DEBE utilizar un tamaño de bloque de 8 octetos (64 bits).

Cuando se requiera relleno, este DEBE ser realizado según las convenciones especificadas en [ESP].

4. Material Clave

DES-CBC es un algoritmo de clave secreta simétrico. El tamaño de la clave es de 64 bits. (Se conoce comúnmente como clave de 56 bits puesto que la clave tiene 56 bits significativos; el bit menos significativo en cada byte es el bit de paridad.)

[arch] describe el mecanismo general para derivar material clave de la transformación ESP. La derivación de la clave de una cierta cantidad de material clave no se diferencia entre asociaciones de seguridad (SA) de clave manual y de clave automática.

Este mecanismo DEBE derivar un valor de clave de 64 bit para utilizarse según ese cifrado. El mecanismo derivará valores de claves en bruto, el proceso de derivación en si mismo no es responsable de manejar paridad o verificaciones de claves débiles.

Las verificaciones de claves débiles DEBERÍA ser realizada. Si se encuentra tal clave, la clave DEBERÍA ser rechazada y una nueva SA se requerirá.

Nota de Implementación:

Si una implementación elige realizar el control de clave débil, esta debería reconocer que claves débiles conocidas [FIPS74] se han normalizado según la paridad. De otro modo el manejo de la paridad es un tema local.

Una función seudo aleatoria fuerte DEBE ser utilizada para generar la clave requerida. Para una discusión sobre este asunto, referirse a [RFC1750].

4.1 Claves Débiles

El DES tiene 16 claves débiles conocidas, incluyendo también las claves llamadas semi-débiles. La lista de claves débiles puede ser encontrada en [FIPS74].

4.2 Tiempo de Vida de las Claves

[Blaze96] discute los costos y el tiempo de recuperación de claves de ataques por fuerza bruta. Presenta varias combinaciones de costo total/tiempo para recuperar una clave/costo por clave recuperada de 40 bit y claves DES de 56 bits, basado en 1995 estimaciones.

Mientras que una búsqueda por fuerza bruta de un espacio de clave DES de 56 bits puede ser considerado impracticable para el hacker, que está utilizando simples ciclos de CPU o otros recursos menos costosos, esto está dentro del alcance de alguien que quiere gastar un poco más de dinero.

Por ejemplo, con un costo de $300.000, una clave DES de 56 bits se puede recuperar aproximadamente en 19 días usando tecnología comercial disponible y solamente 3 horas usando un chip desarrollado a pedido.

Se debe observar que hay otros ataques que pueden recuperar claves más rápido, los ataques por fuerza bruta están considerados como los de la "peor clase", aunque son los más fácil de implementar.

[Wiener94] también discute una máquina de $1M que puede romper una clave DES en 3.5 horas (1993 estimaciones), empleando un ataque a un texto plano conocido. Según lo discutido en la sección Consideraciones de Seguridad, un ataque a un texto plano conocido es razonablemente probable.

Se debe observar que con el correr del tiempo los costos de búsqueda total y/o parcial, así como también el tipo de recuperación parcial de clave seguirán disminuyendo.

Mientras que lo antedicho no proporciona recomendaciones específicas para el tiempo de vida de la clave, esto refuerza el punto que para una aplicación dada el tiempo de vida de la clave deseada es dependiente de la amenaza percibida (una conjetura adecuada en cuanto a la cantidad de recursos disponibles del atacante) concernientes al valor de los datos que se protegerán.

Mientras que no hay recomendaciones para el tiempo de vida basados en volúmenes de tráfico hechos aquí, se debería observar que dado el suficiente volumen de tráfico habrá mayor probabilidad de que el texto plano conocido pueda ser acumulado.

5. Interacción con Algoritmos de Autentificación

Al momento de la creación de este documento, no hay temas que imposibiliten el uso del algoritmo DES-CBC con algún algoritmo específico de autentificación.

6. Consideraciones de Seguridad

(Gran parte de esta sección fue escrita originalmente por Guillermo Allen Simpson y Perry Metzger.)

Los usuarios necesitan entender que la calidad de seguridad proporcionada por esta especificación depende completamente de la fuerza del algoritmo DES, la exactitud de implementación de esos algoritmos, la seguridad del mecanismo de administración de Asociación de Seguridad y de su implementación, de la fuerza de la clave [CN94], y la exactitud de las implementaciones en todos los nodos que participan.

[Bell95] y [Bell96] describen un ataque empleando cortar y pegar que se aplica a todos los algoritmos de Encadenamiento de Bloque Cifrado. Este ataque se puede solucionar con el uso de mecanismos de autentificación.

El uso de mecanismos de encriptación sin ningún mecanismo de autentificación no se recomienda. Este cifrado puede ser utilizado en una transformación ESP que también incluya autentificación; esto también puede ser utilizado en una transformación ESP que no proporcione autentificación incluida (en ESP) pero hay una cabecera AH (proporcionando autentificación). Referirse a [ESP], [AH], [arch], y a [Road] para más detalles.

Cuando el relleno de ESP es utilizado, los bytes de relleno tienen un valor previsible. Proporcionando una pequeña cantidad de detección de sabotaje (tamper) sobre su propio bloque y sobre el bloque anterior

en modo CBC. Esto hace que sea un poco más difícil realizar ataques uniendo (splicing) y evitando un posible canal secreto. Esta pequeña cantidad de texto plano conocido no crea ningún problema para los cifrados modernos.

Cuando se creó este documento, [BS93] demostró un criptoanálisis diferencial basado en la elección del texto plano, el ataque requerirá 2^47 pares de texto plano-texto cifrado, donde el tamaño de un par es el tamaño de un bloque DES (64 bits). [Matsui94] demostró un criptoanálisis lineal basado en la elección del texto plano conocido, el ataque solamente requería 2^43 pares de; texto plano, texto cifrado. Aunque estos ataques no son considerados prácticos, se deben tener en cuenta.

Más perturbadora mente, [Wiener94] muestra el diseño de una máquina de cracking para DES que costaba $1 millones que pueden craquear una clave cada 3,5 horas. Esto es un ataque extremadamente práctico.

Uno o dos bloques de texto plano conocido son suficientes para recuperar una clave DES. Debido a que los datagramas IP comienzan típicamente con un bloque de texto conocido y/o predecible de la cabecera, los cambios frecuentes de clave no protegerán contra este ataque.

Se sugiere que el DES no es un buen algoritmo de encriptación para la protección de información de valor moderado frente a tal equipo. El triple DES es probablemente una mejor opción para tales propósitos.

Sin embargo, a pesar de estos riesgos potenciales, el nivel de privacidad proporcionado por ESP con DES-CBC es mayor que enviar el datagrama en texto plano a través de Internet.

El caso para usar los valores aleatorios para los IV sse ha refinado el siguiente resumen proporcionado por Steve Bellovin. Referirse a [Bell97] para mayor información.

"El problema se presenta si usted utiliza un contador como IV, o otra fuente con una distancia de Hamming baja entre sucesivos IV, para la encriptación en modo CBC. En modo CBC, el "texto plano efectivo" para una encriptación es el XOR del texto plano actual y del texto cifrado del bloque precedente. Normalmente, ese es un valor aleatorio, que significa que el texto plano efectivo es algo aleatorio. Eso es no cambian mucho entre paquetes.

Para el primer bloque del texto plano el IV toma el lugar del bloque anterior del texto cifrado. Si el IV no se diferencia mucho del IV anterior, y el bloque actual del texto plano no se diferencia mucho del paquete anterior, entonces el texto plano efectivo tampoco se favorable, debido a que muchos de los bloques de texto plano actual

diferenciará mucho. Esto significa que usted tiene pares de bloques de texto cifrado combinados con los bloques de texto plano que se diferencian en apenas algunas posiciones de bits. Esto puede ser una ventaja [wedge] para los diversos ataques criptográficos."

La discusión sobre los IV se ha actualizado para requerir que una implementación no use una fuente de distancia de Hamming baja para los IV.

7. Referencias

[Bell95] Bellovin, S., "An Issue With DES-CBC When Used Without Strong Integrity", Presentation at the 32nd Internet Engineering Task Force, Danvers Massachusetts, April 1995.

[Bell96] Bellovin, S., "Problem Areas for the IP Security Protocols", Proceedings of the Sixth Usenix Security Symposium, July 1996.

[Bell97] Bellovin, S., "Probable Plaintext Cryptanalysis of the IP Security Protocols", Proceedings of the Symposium on Network and Distributed System Security, San Diego, CA, pp. 155-160, February 1997 (also http://www.research.att.com/~smb/papers/probtxt.{ps, pdf}).

[BS93] Biham, E., and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Berlin: Springer-Verlag, 1993.

[Blaze96] Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E., and M. Wiener, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security", currently available at http://www.bsa.org/policy/encryption/cryptographers.html

[CN94] Carroll, J.M., and S. Nudiati, "On Weak Keys and Weak Data: Foiling the Two Nemeses", Cryptologia, Vol. 18 No. 23 pp. 253-280, July 1994.

[FIPS-46-2] US National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 46-2, December 1993, http://www.itl.nist.gov/div897/pubs/fip46-2.htm (supercedes FIPS-46-1).

[FIPS-74] US National Bureau of Standards, "Guidelines for Implementing and Using the Data Encryption Standard", Federal Information Processing Standard (FIPS) Publication 74, April 1981, http://www.itl.nist.gov/div897/pubs/fip74.htm.

[FIPS-81] US National Bureau of Standards, "DES Modes of Operation", Federal Information Processing Standard (FIPS) Publication 81, December 1980, http://www.itl.nist.gov/div897/pubs/fip81.htm.

[Matsui94] Matsui, M., "Linear Cryptanalysis method for DES Cipher", Advances in Cryptology -- Eurocrypt '93 Proceedings, Berlin: Springer-Verlag, 1994.

[RFC-1750] Eastlake, D., Crocker, S., and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

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

[Schneier96] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1996. ISBN 0-471-12845-7.

[Wiener94] Wiener, M.J., "Efficient DES Key Search", School of Computer Science, Carleton University, Ottawa, Canada, TR-244, May 1994. Presented at the Rump Session of Crypto '93. [Reprinted in "Practical Cryptography for Data Internetworks", W.Stallings, editor, IEEE Computer Society Press, pp.31-79 (1996). Currently available at ftp://ripem.msu.edu/pub/crypt/docs/des-key-search.ps.]

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

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

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

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

8. Agradecimientos

Mucha de la información proporcionada aquí originada con los diversos documentos de ESP-DES realizados por Perry Metzger y Guillermo Allen Simpson, especialmente la sección Consideraciones de Seguridad.

Este documento también es derivado en parte de trabajos previos realizados por Jim Hughes, como así también de las personas que trabajaron con Jim en el DES-CBC+HMAC-MD5 combinado con ESP transforme, los participantes del bakeoff de ANX, y los miembros del grupo de trabajo de IPsec.

Gracias a Rob Glenn por asistir con el formato del nroff.

El grupo de trabajo de IPsec puede ser contactado vía lista de correo del grupo de trabajo de IPsec (ipsec@tis.com) o a través de sus autoridades:

Robert Moskowitz
International Computer Security Association
EMail: rgm@icsa.net
Theodore Y. Ts'o
Massachusetts Institute of Technology
EMail: tytso@MIT.EDU

9. Direcciones de los Autores

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

Naganand Doraswamy
Bay Networks, Inc.
EMail: naganand@baynetworks.com

10. Declaración de Copyright Completa

Notas del Traductor

El significado y/o definición de las siguientes palabras del ingles y/o español es:

- Distancia de Hamming: El número de las posiciones de dígito en las cuales los dígitos correspondientes de dos palabras binarias de la misma longitud son diferentes. Nota 1: La distancia de Hamming entre 1011101 y 1001001 es dos. Nota 2: El concepto se puede ampliar a otros sistemas de la notación. Por ejemplo, la distancia de Hamming entre 2143896 y 2233796 es tres. (según: ITS-Institute for Telecommunication Sciences)

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.

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