Noviembre 1998
Request for Comments: 2410
Categoría: Pila de Estándares

R. Glenn
NIST
S. Kent
BBN Corp

November 1998

Traducción al castellano:
Agosto 2005

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

El uso del Algoritmo de Encriptación NULL y su uso con IPsec

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 define el algoritmo de encriptación NULL y su uso con la Carga de Seguridad Encapsulada [ESP] de IPsec. NULL no altera los datos del texto plano. En realidad, NULL, por si mismo, no hace nada. NULL proporciona los medios para que ESP proporcione autentificación y integridad sin confidencialidad.

La información adicional sobre otros componentes necesarios para las implementaciones ESP se proporcionan en [ESP] y [ROAD].

1. Introducción

Este documento define el algoritmo de encriptación NULL y su uso con la Carga de Seguridad Encapsulada [ESP] de IPsec para proporcionar autentificación y integridad sin confidencialidad.

NULL es un bloque cifrado cuyos orígenes parecen estar perdidos en la antigüedad. A pesar de los rumores de que la Agencia de Seguridad Nacional omitió la publicación de este algoritmo, no hay evidencia de esta acción. Mas bien, evidencia arqueológica reciente sugiere que el algoritmo NULL fue desarrollado en tiempos romanos, como un

alternativa exportable para los cifrados del César. Sin embargo porque los números romanos carece de un símbolo para el numero cero, algoritmo NULL fue desarrollado en tiempos romanos, como un alternativa exportable para los cifrados del César. Sin embargo porque los números romanos carece de un símbolo para el numero cero, registros manuscritos del desarrollo del algoritmo estuvieron perdidos para los historiadores por mas de dos milenios.

[ESP] especifica el uso de un algoritmo de encriptación opcional para proporcionar confidencialidad y el uso de un algoritmo de autentificación opcional para proporcionar autentificación y integridad. El algoritmo de encriptación NULL es un modo conveniente de representar la opción de no aplicar encriptación. Esto es referido como ESP_NULL en [DOI].

La especificación de la cabecera de Autentificación [AH] proporciona un servicio similar, el cálculo de los datos de autentificación cubre, la parte de datos de un paquete, como así también las partes que no se modifican durante el trasporte en la cabecera IP. ESP_NULL no incluye la cabecera IP en el cálculo de los datos de autentificación. Esto puede ser útil para proporcionar servicios IP a través de dispositivos de redes no IP. La discusión de como ESP_NULL debería ser usado con dispositivos de redes no IP esta fuera del alcance de este documento.

En este documento, NULL esta usado dentro del contexto de ESP. Para información adicional de cómo varias partes de ESP se unen para proporcionar servicios de seguridad, referirse a [ESP] y a [DOI].

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. Definición del Algoritmo

NULL esta matemáticamente definido por el uso de la función Identidad I aplicada a un bloque de datos b tal que:

$$NULL(b) = I(b) = b$$

2.1 Material Clave

Así como otros cifrados modernos, por ejemplo RC5 [RFC-2040], el algoritmo de encriptación NULL puede hacer uso de claves de longitud variable. Sin embargo no existe un incremento cuantificable de seguridad mediante el uso de longitudes de claves mas largas.

2.2 Sincronización criptográfica

Debido a la naturaleza desnacionalizada del algoritmo de encriptación NULL no es necesario trasmitir un IV o datos de sincronización criptográficos similares en cada paquete básico (o por cada SA). El algoritmo de encriptación NULL combina muchas de las mejores características del encadenamiento de bloque cifrado y del encadenamiento de flujo cifrado mientras que todavía no requiere la transmisión de un IV o datos de sincronización criptográficos análogos.

2.3 Relleno

NULL tiene un tamaño de bloque de 1 byte, de esa manera el relleno no es necesario.

2.4 Funcionamiento

El algoritmo de encriptación NULL es significativamente mas rápido que otros algoritmos de encriptación simétricos y las implementaciones del algoritmo base están disponibles para todo hardware y plataformas de Sistemas Operativos.

2.5 Vectores de Prueba

Los siguiente es un conjunto de vectores de prueba para facilitar el desarrollo de interoperatibilidad de implementaciones NULL.

```
test_case =      1
data =           0x123456789abcdef
data_len =       8
NULL_data =      0x123456789abcdef

test_case =      2
data =           "Network Security People Have A Strange Sense Of Humor"
data_len =       53
NULL_data =      "Network Security People Have A Strange Sense Of Humor"
```

3. Requisitos operacionales de ESP_NULL

ESP_NULL esta definido por el uso de NULL dentro del contexto de ESP. Esta sección define ESP_NULL explicando los requisitos particulares de parámetros operacionales.

Para los propósitos de extracción de clave de IKE [IKE], el tamaño de la clave para este algoritmo DEBE ser de cero bits (0), para facilitar la interoperatibilidad y para evitar problemas potenciales de control de exportación.

Para facilitar la interoperatibilidad, el tamaño del IV para este algoritmo debe ser de cero (0) bits.

El relleno PUEDE ser incluido en paquetes salientes como esta especificado en [ESP].

4. Consideraciones de seguridad

El algoritmo de encriptación NULL no ofrece confidencialidad ni cualquier otro servicio de seguridad. Es simplemente un modo conveniente de representar el uso opcional de aplicar encriptación dentro de ESP. Por lo tanto ESP puede ser usado para proporcionar autentificación y integridad sin confidencialidad. Diferente a AH, estos servicios no son aplicados a ninguna parte de la cabecera IP. Al momento de la creación de este documento no hay evidencia para decir que ESP_NULL es menos seguro que AH cuando se usa el mismo algoritmo de autentificación (es decir un paquete asegurado usando ESP_NULL con algún algoritmo de autentificación es tan seguro criptográficamente hablando como un paquete aseguradon usado AH con el mismo algoritmo de autentificación).

Como está indicado en [ESP], mientras que el uso de algoritmos de encriptación y de autentificación son opcionales en ESP, es imperativo que una SA ESP especifique, el uso de al menos un algoritmo de encriptación criptográficamente fuerte o un algoritmo de autentificación criptográficamente fuerte o uno de cada uno.

Al momento de la redacción de este documento no existen leyes conocidas que impidan la exportación de NULL con una longitud de clave de cero (0) bits.

5. Derechos de propiedad intelectual

Conforme a las provisiones del [FRC-2026] los autores representan que han divulgado la existencia de cualquier derecho de propiedad o derecho de propiedad intelectual en la contribución que es racionalmente y personalmente conocida para los autores. Los autores no representan que ellos conozcan personalmente la propiedad pertinente y los derechos de propiedad intelectual reclamados por las organizaciones que ellos representan o terceras partes.

6. Agradecimientos

Steve Bellovin sugirió y proporcionó el texto de la sección derecho de propiedad intelectual.

El crédito también necesita ser dado a los participantes del grupo de trabajo de interoperatibilidad Cisco/ICSA IPsec & IKE March 1998 puesto que fue allí que la necesidad de este documento se convirtió en necesaria.

7. Referencias

[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.

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

[DOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2408, November 1998.

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

[RFC-2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC-2040] Baldwin, R., and R. Rivest, "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms", RFC 2040, October 1996

[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

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

Stephen Kent
BBN Corporation
EMail: kent@bbn.com

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

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