Grupo de Trabajo en Red
Request for Comments: 2411
Categoría: Informativo

R. Thayer
Sable Technology Corporation
N. Doraswamy
Bay Networks
R. Glenn
NIST

Noviembre 1998

Traducción al castellano:
Hugo Adrian Francisconi

Agosto 2005

<adrianfrancisconi@yahoo.com.ar>

# Documento de Guía para IPsec

## Estado de este documento



## Aviso de Copyright



## Resumen

El conjunto de protocolos IPsec se utiliza para proporcionar servicios de privacidad y autentificación en la capa IP. Muchos documentos se utilizan para describir este conjunto de protocolos. La interrelación y la organización de varios documentos que cubren el protocolo IPsec se discuten aquí. Una explicación de que encontrar en cada documento y que incluir en un nuevo algoritmo de encriptación y algoritmo de autentificación también se describen aquí.

## Lista de contenido

## 1. Introducción

Este documento tiene la intención de proporcionar recomendaciones para el desarrollo de especificaciones colaterales que describen el uso de nuevos algoritmos de autentificación y encriptación con el protocolo ESP, descripto en [ESP] y nuevos algoritmos de autentificación usados con el protocolo AH, descriptos en [AH]. ESP y AH son parte de la Arquitectura de Seguridad IP descripta en [Arch]. Existe un requisito para un procedimiento bien conocido que puede ser usado para agregar nuevos algoritmos de encriptación o autentificación para ESP y AH, no solamente mientras el conjunto de documento inicial está en desarrollo sino también después que los documentos base hayan alcanzado el estatus de RFC. Las siguientes recomendaciones que se discuten debajo simplifican el agregado de nuevos algoritmos y reduce la cantidad de documentación redundante.

El objetivo de escribir un nuevo documento de algoritmos de encriptación o autentificación es para concentrarse en la aplicación de un algoritmo específico dentro de ESP y AH. Los conceptos generales de ESP y AH, definiciones, y cuestiones relacionadas son cubiertas en los documentos ESP y AH. Los algoritmos no están descriptos en estos documentos. Esto nos da la capacidad para agregar nuevos algoritmos y también para especificar cómo cualquier algoritmo dado puede interactuar. La idea es alcanzar el objetivo de eludir la duplicación de información y el número de documentos excesivos, el efecto llamado "explosión de borradores".

## 2. Interrelación de Documentación sobre IPsec

Los documentos que describen el conjunto de protocolos IPsec se dividen en siete grupos. Esto se ilustra en el cuadro 1. Hay un documento principal de arquitectura que cubre ampliamente el concepto general, requerimientos de seguridad, definiciones, y mecanismos que definen la tecnología IPsec.

Hay un documento del Protocolo ESP y un documento del Protocolo AH que describe el formato del paquete y asuntos generales con respecto a estos protocolos. Estos documentos del protocolo también contienen valores por defecto si es apropiado, por ejemplo, los contenidos de relleno por defecto, y los algoritmos que obligatoriamente deben ser implementados. Estos documentos dictan algunos de los valores del documento Dominio de Interpretación [DOI]. Observe que el documento

DOI es parte del mecanismo de Asignación de Números de IANA y por ende los valores descriptos en el DOI deben ser bien conocidos. Vea [DOI] para más información sobre el mecanismo.

El conjunto de documentos de "Algoritmos de Encriptación", mostrados abajo, es el conjunto de documentos que describen cómo varios algoritmos de encriptación son utilizados por ESP. Estos documentos están realizados con la intención de adaptarse a esta guía básica, y se debería evitar superponerse con el documento del protocolo ESP y con los documentos de los Algoritmos de Encriptación. Ejemplos de estos documentos son [DES-Detroit] y [CBC]. Cuando éstos u otros algoritmos de encriptación se utilizan para ESP, el documento del DOI tiene que indicar ciertos valores, tales como un identificador de algoritmo de encriptación, por ende estos documentos proporcionan información al DOI.

El conjunto de documentos de "Algoritmos de Autentificación", mostrados abajo, es el conjunto de documentos que describen cómo varios algoritmos de autentificación son utilizados por ESP y AH. Estos documentos están realizados con la intención de adaptarse a esta guía básica, y se debería evitar superponerse con el documento del protocolo AH y con los documentos de los Algoritmos de Autentificación. Ejemplos de estos documentos son [HMAC-MD5] y [HMAC-SHA-1]. Cuando éstos u otros algoritmos de encriptación se utilizan para ESP o AH, el documento del DOI tiene que indicar ciertos valores, tales como el tipo de algoritmo, por ende estos documentos proporcionan información al DOI.

Los documentos de "Administración de Claves", como se muestran en la figura, son los documentos que describen los esquemas de administración de clave de los delineamientos estándares de ITEF. Estos documentos también proporcionan ciertos valores para el DOI. Observe que las aplicaciones de administración de claves deben ser indicadas aquí y no por ejemplo, en los documentos del protocolo ESP y AH. Esta figura representa [ISAKMP], [Oakley], y [Resolution].

El documento DOI, como se muestra en la figura, contiene valores necesarios para que otros documentos se relacionen entre si. Esto incluye por ejemplo algoritmos de encriptación, algoritmos de autentificación, y parámetros operacionales como tiempos de vida de la claves.

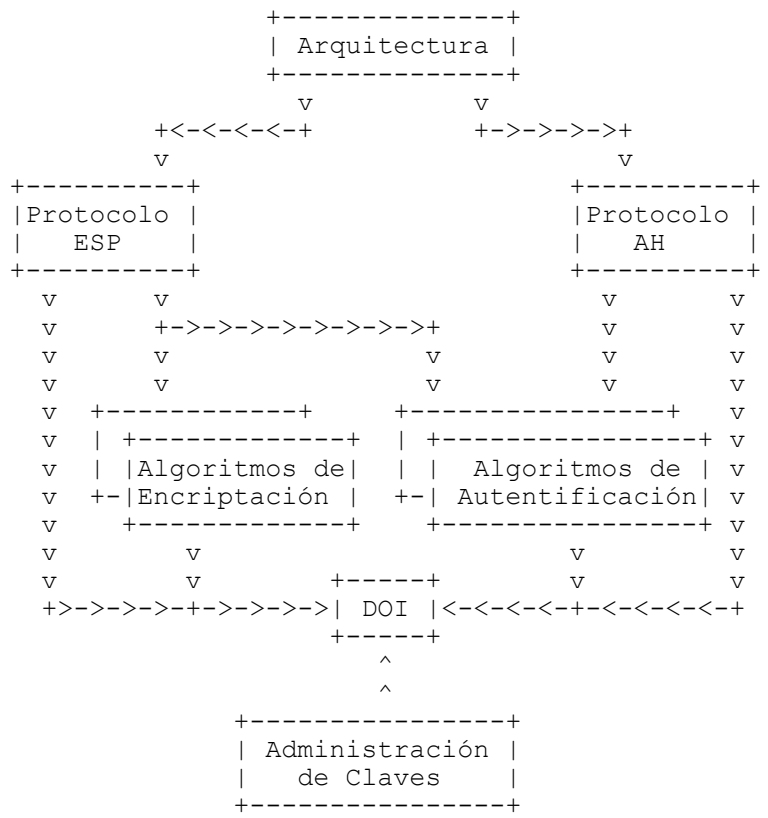


Figura 1: Documentación guía de IPsec

## 3. Material Clave

Describir los algoritmos de encriptación y de autentificación en diferentes documentos plantea cómo los protocolos de administración de claves conocen la longitud del material clave requerido para los algoritmos deseados cuando se usan junto con ESP. También plantea la cuestión de cómo dividir el material clave. Esto se conoce como "slicing and dicing".

Cada documento de Algoritmo de Encriptación y de Algoritmo de Autentificación debería especificar sus respectivos atributos de clave (por ejemplo, cómo rellenar, la localización de los bits de paridad, el orden de la clave para los algoritmos de clave-múltiple, y longitud). Los protocolos de administración de claves deberían utilizar la longitud de las claves especificadas en los respectivos

documentos de los Algoritmos para generar el material clave de longitud requerida.

El protocolo de administración de claves genera material clave con bastante fuerza y tamaño para generar las claves para los algoritmos individuales. El documento de la Arquitectura de IPsec específica cómo las claves se extraen de un único bloque de material clave cuando se requieren múltiples claves (por ejemplo, ESP con autentificación). Los documentos de Algoritmo de Encriptación y de Algoritmo de Autentificación son responsables de especificar los tamaños de las claves y las fuerzas de cada algoritmo. Sin embargo, si el material clave entero se pasa al kernel para realizar slicing and dicing o si las claves son sliced y diced por el protocolo de administración de claves es una cuestión de implementación. El documento del protocolo AH no tiene tal requerimiento.

## 4. Contenido Recomendado de Documentación sobre Algoritmos

Este documento describe cómo un algoritmo de encriptación o autentificación usado debe contener información apropiada para ese algoritmo de encriptación o autentificación. Esta sección enumera que información debe ser proporcionada. La intención de la guiá básica del documento es que:

- La información general del protocolo de los documentos respectivos ESP o AH.
- La información de administración de claves este en los documentos de administración de claves.
- Los valores asignados y las constantes de los ítems negociables estén en el documento de DOI.

Los algoritmos de encriptación y de autentificación requieren un cierto conjunto opcional de parámetros o tienen modos de operación opcionales (por ejemplo, el IV, la longitud de los datos de autentificación, y longitud de las claves). Para ayudar a eliminar cierta complejidad relacionada con la administración de claves que tienen que negociar números extensos de parámetros de algoritmos específicos, los documentos de algoritmos de autentificación y encriptación seleccionarán valores fijos para estos parámetros cuando se estime técnicamente razonable y accesible.

Observe que la siguiente información intenta ser solamente una pauta general.

### 4.1 Algoritmos de Encriptación y Autentificación

Esta sección describe la información que debe ser incluida en los

documentos de Algoritmos de Encriptación y Algoritmos de Autentificación.

Material Clave

. Tamaño de las claves, incluyendo tamaños mínimos, máximos, recomendados y/o requeridos. Observe que la sección de consideraciones de seguridad debe tratar cualquier debilidad en los tamaños específicos.
. Las técnicas recomendadas o requeridas de generación de números seudo aleatorios y los atributos para proporcionar claves suficientemente fuertes. [RANDOM] proporciona recomendaciones sobre la generación de aleatoriedad fuerte para el uso de seguridad.
. Formato del material clave.
. Claves débiles conocidas o referencias de la documentación de claves débiles conocidas.
. El proceso recomendado o requerido para la entrada de material clave tal como la generación de paridad o control.
. Requisitos y/o recomendaciones sobre con que frecuencia el material clave debe ser renovado.

Consideraciones del Funcionamiento
. Estimaciones disponibles sobre el funcionamiento de este algoritmo.
. Datos de comparación disponible (por ejemplo, comparado con DES o MD5).
. El tamaño de la entrada u otras consideraciones que podrían mejorar o degradar el funcionamiento.

Consideraciones del Entorno ESP
. Cualquier cuestión conocida con relación a las interacciones entre este algoritmo y otros aspectos de ESP, tales como el uso de ciertos esquemas de autentificación. Observe: Así como los nuevos algoritmos de encriptación y autentificación se aplican a ESP, los más recientes documentos serán requeridos para tratar interacciones con algoritmos previamente especificados.

Contenido de la Carga y Descripción del Formato
. Especificación del tamaño, ubicación y contenido de los campos del algoritmo específico no definido en los documentos de los protocolos de ESP o AH (por ejemplo IV).

Consideraciones de Seguridad
. Discutir cualquier ataque conocido.
. Discutir cualquier dificultad común de implementación, tal como el uso de generadores aleatorios de números débiles.
. Discutir cualquier procedimiento relevante a la validación, tal como vectores de prueba. [RFC-2202] es un documento de ejemplo que

contiene vectores de prueba para un conjunto de algoritmos de autentificación.

## 4.2 Algoritmos de Encriptación

Esta sección describe la información que debe ser incluida en los documentos de Algoritmos de Encriptación.

Descripción del Algoritmo de Encriptación
. Información general de cómo este algoritmo de encriptación debe ser utilizado en ESP
. Descripción del material de base y descripción formal del algoritmo.
. Características de este algoritmo de encriptación que se utilizará en ESP, incluyendo encriptación y/o autentificación.
. Mención de cualquier cuestión de disponibilidad tales como las consideraciones de Propiedad Intelectual.
. Referencias, según el IETF, para el material de base tal como los documentos FITS.

Modo de Operación del Algoritmo
. Descripción de cómo funciona el algoritmo, si es en modo bloque o en modo encadenamiento (flujo) u otro.
. Requisitos para el formato de bloques de entrada o salida de información.
. Requisitos del relleno de este algoritmo. Observe que hay un valor por defecto para el relleno, especificado en el documento base ESP, por lo tanto esto es necesario si el valor por defecto no puede ser utilizado.
. Cualquiera de los parámetros operativos del algoritmo específico, tales como número de ciclos.
. Determinar parámetros opcionales y métodos de operación opcionales y elegir valores fijos razonables y métodos con explicaciones técnicas explícitas.
. Determinar los parámetros opcionales en los cuales los valores y los métodos deben seguir siendo opcionales con explicaciones técnicas explícitas en las que los valores y métodos fijos no deben ser utilizados.
. Valores por defecto y rangos obligatorios en los parámetros opcionales de algoritmos específicos que no podrían ser fijos.

## 4.3 Algoritmos de Autentificación

Esta sección describe la información que debe ser incluida en los documentos de Algoritmos de Autentificación. En la mayoría de los casos, un algoritmo de autentificación operará igual si es usado para ESP o AH. Esto debe ser presentado en un único documento de Algoritmo de Autentificación.

Descripción del Algoritmo de Autentificación
. Información general de cómo este algoritmo de autentificación debe ser utilizado en AH y ESP.
. Descripción del material de base y descripción formal del algoritmo.
. Características de este algoritmo de autentificación.
. Mención de cualquier cuestión de disponibilidad tales como las consideraciones de Propiedad Intelectual.
. Referencias, según el IETF, para el material de base tal como los documentos FITS y descripciones definitivas de algoritmos subyacentes.

Modo de Operación del Algoritmo
. Descripción de cómo funciona el algoritmo.
. Parámetros operativos del algoritmo específico tal como el número de ciclo, formato del bloque de entrada y de salida.
. Requisitos del relleno implícito y explicito de este algoritmo. Observe que hay un método por defecto para el relleno del campo de datos de autentificación especificado en un documento de protocolo AH. Esto solamente es necesario si el valor por defecto no puede ser usado.
. Identificar parámetros opcionales y métodos opcionales de operación y elegir valores fijos razonables y métodos con explicaciones técnicas explicitas.
. Determinar parámetros opcionales y métodos de operación opcionales y elegir valores fijos razonables y métodos con explicaciones técnicas explícitas.
. Determinar los parámetros opcionales en los cuales los valores y los métodos deben seguir siendo opcionales con explicaciones técnicas explícitas en las que los valores y métodos fijos no deben ser utilizados.
. Valores por defecto y rangos obligatorios en los parámetros opcionales del algoritmo específico que no podrían ser fijos.
. Criterios de comparación de los datos de Autentificación para este algoritmo. Observe: hay un método por defecto para verificar los datos de autentificación especificados en el documento del protocolo AH. Esto es solamente necesario si el valor por defecto no puede ser usado (por ejemplo, cuando es utilizado en un hash firmado).

## 5. Consideraciones de Seguridad

Este documento proporciona una guía básica y directivas para la redacción de los documentos de algoritmos de encriptación y de autentificación. El lector debe seguir todos los procedimientos de seguridad y directivas descriptas en la Arquitectura de Seguridad, Protocolo ESP, Protocolo AH, y documentos de los algoritmos de

autentificación y encriptación. Observe que muchos de los algoritmos de encriptación no son considerados seguros si no están usados con un cierto mecanismo de autentificación.

## 6. Agradecimientos

Varios bosquejos de Internet fueron referidos al escribir este documento. Dependiendo de donde los documentos estén en ITEF, los documentos podrían no estar disponibles a través de los repositores ITEF RFC. En ciertos casos el lector puede desear saber a que versión de estos documentos se hizo referencia. Estos documentos son:

. DES-Detroit: éste es el estilo ANX de trabajo de ESP, basado en el bosquejo de Hughes según lo modificado por Cheryl Madson y publicado en la lista ANX.
. DOI: draft-ietf-ipsec-ipsec-doi-02.txt.
. 3DES: éste es el <documento del Triple-DES>.
. CAST: éste es draft-ietf-ipsec-esp-cast-128-cbc-00.txt, según lo revisado para relacionarse con este documento.
. ESP: draft-ietf-ipsec-esp-04.txt, enviado a la lista del IETF en mayo/el junio de 1997.
. AH: draft-ietf-ipsec-auth-05.txt, enviado a la lista del IETF en mayo/el junio de 1997.
. HUGHES: éste es draft-ietf-ipsec-esp-des-md5-03.txt
. ISAKMP: Hay tres documentos que describen el ISAKMP. Éstos son draft-ietf-ipsec-isakmp-07.txt, draft-ietf-ipsec-isakmp-oakley-03.txt, y draft-ietf-ipsec-ipsec-doi-02.txt.

## 7. Referencias

[CBC] Periera, R., and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

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

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

[DOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

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

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

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

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

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

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

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

## 8. Dirección de los Autores

Rodney Thayer
Sable Technology Corporation
246 Walnut Street
Newton, Massachusetts 02160
EMail: mailto:rodney@sabletech.com

Naganand Doraswamy
Bay Networks
EMail: naganand@baynetworks.com

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

## 9. Declaración de Copyright Completa

Estándares Internet, o con motivo de su traducción a otras lenguas aparte del Inglés.

Los limitados permisos concedidos arriba son perpetuos y no serán revocados por la Internet Society ni sus sucesores o destinatarios.

Este documento y la información contenida en él se proporcionan en su forma "TAL CUAL" y LA INTERNET SOCIETY Y LA INTERNET ENGINEERING TASK FORCE RECHAZAN CUALESQUIERA GARANTIAS, EXPRESAS O IMPLICITAS, INCLUYENDO, PERO NO LIMITADAS A, CUALQUIER GARANTIA DE QUE EL USO DE LA INFORMACION AQUI EXPUESTA NO INFRINGIRA NINGUN DERECHO O GARANTIAS IMPLICITAS DE COMERCIALIZACION O IDONEIDAD PARA UN PROPOSITO ESPECIFICO.

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.

La referencia [Resolution] descripta en este RFC (RFC 2411) hace referencia al RFC 2409 (IKE) pero al autor parece ser que se le olvidó referenciarlo en la Sección 7 (Referencias). Como así también la referencia [ISAKMP] descripta en este RFC (RFC 2411) hace referencia al RFC 2408 (ISAKMP) pero al autor parece ser que se le olvidó referenciarlo en la Sección 7.

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.

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