

CCP.I/RES. 46 (IV-04)¹

ARQUITECTURA DE SEGURIDAD PARA EL PROTOCOLO DE INTERNET

La IV Reunión del Comité Consultivo Permanente I: Normalización de Telecomunicaciones,

CONSIDERANDO:

- a) Que con el desarrollo de las tecnologías de comunicación e información, las redes de comunicación e información han dado origen a retos de seguridad cada vez mayores;
- b) Que el documento IETF RFC 2401 “Arquitectura de seguridad para el protocolo de Internet” es un marco de normas abiertas que ofrece seguridad para la transmisión de información sensible a través de redes sin protección tales como Internet; y
- c) Que el IETF RFC 2401 da soporte a diferentes aplicaciones, que van desde la capacidad de comunicación de banda estrecha a comunicación de banda ancha con movilidad personal y de terminal integrada para satisfacer los requerimientos del usuario y servicio,

RECONOCIENDO:

- a) Que los operadores de telecomunicaciones y los proveedores de servicio de la región enfrentan amenazas de seguridad de una amplia gama de fuentes, incluyendo fraudes asistidos por computador, espionaje, sabotaje, vandalismo, etc.; y
- b) Que las fuentes de daño como virus informáticos, piratería informática y ataques de negación de servicio se han vuelto más comunes, más ambiciosos y cada vez más sofisticados,

RESUELVE:

Adoptar la IETF RFC 2401 “Arquitectura de seguridad para el protocolo de Internet” sin supresiones, adiciones o modificaciones.

RECOMIENDA:

- 1. Que el Grupo de Trabajo sobre Coordinación de Normas continúe el monitoreo y determine el alcance en las Américas de la norma IETF RFC 2401 conforme evolucione; y
- 2. Que el Grupo de Trabajo sobre Coordinación de Normas continúe abordando las necesidades de servicio de las Américas y suministre opciones de implementación basándose en IETF RFC 2401 y otras normas en desarrollo de seguridad de redes.

¹ CCP.I-TEL/doc.428/04

ANEXO A LA RESOLUCION CCP.I/RES. 46 (IV-04)

Documento Coordinado de Normas Arquitectura de Seguridad para el Protocolo de Internet

1. RESUMEN EJECUTIVO

Internet y demás redes de comunicación son una parte cada vez más importante en nuestras vidas diarias, al igual que nuestra dependencia en su infraestructura subyacente. Desafortunadamente, junto con nuestra dependencia han crecido los ataques hostiles en la infraestructura por parte de los depredadores de redes. Las formas de ataque descubiertas recientemente, la disponibilidad y distribución masiva de herramientas de ataque, así como las fallas en los programas comunes de computadora han provocado que las redes resulten cada vez más vulnerables.

La flexibilidad y fortaleza del IP constituyen también su debilidad; la forma en que el IP enruta los paquetes facilita los ataques como interceptación (en la que una máquina enmascara a otra), intrusión (en la que una transmisión es monitoreada) o secuestro de una sesión en la que el atacante utiliza ambas técnicas para asumir la personalidad de alguna de las partes de la comunicación.

La importancia de seguridad está reconocida tanto por el IETF (Grupo Especial sobre Ingeniería de Internet) como por el UIT-T. Es necesario entender a fondo todas sus cuestiones e implicaciones. Para abordar la Seguridad, el IETF creó el Área de Seguridad y posteriormente la dividió en grupos de trabajo. La Comisión de Estudio 17 del UIT-T (Redes de Datos y Soporte Lógico de Telecomunicaciones) tiene un grupo de estudio de seguridad que se orienta a temas de seguridad en todos los niveles. El papel de cada organización es de alguna manera diferente; el papel principal del Grupo Asesor del Área de Seguridad del IETF es ayudar a los grupos de trabajo del IETF para proveer seguridad en los protocolos que diseñan. El UIT-T se está enfocando en la necesidad de un enfoque global para la difusión de información relacionada con la seguridad de infraestructuras críticas de redes y formas de estimular la cooperación internacional o regional con relación a las infraestructuras críticas de redes.

El conjunto de protocolos de Seguridad IP (IPSec) del IETF, provee seguridad para el tráfico IP en el nivel de red. El Grupo de Trabajo sobre Coordinación de Normas (WGSC) inició el estudio de IPSec (CCP.I/doc. 1518/02) en la XVI reunión del CCP.I realizada en Montevideo, Uruguay en mayo de 2002; la Sección 6 del documento Visión General de Redes de Próxima Generación (CCP.I-TEL/doc. 112/03) ofrece una descripción de IPSec.

2. ANTECEDENTES

Generalidades de IETF RFC 2401

IPSec se describe en RFC 2401 – Arquitectura de seguridad para el Protocolo de Internet [1]. El conjunto de protocolos ofrece los cinco componentes descritos a continuación.

Asociaciones de Seguridad (SAs)

La función de las SAs es proveer un método para que dos partes puedan intercambiar datos de manera segura y las dos partes tengan que concordar con los parámetros de seguridad. Las “SAs” están definidas para tráfico de una sola vía únicamente, por lo tanto para tráfico bidireccional se requiere la definición de dos “SAs”. La SA IPSec especifica los siguientes parámetros:

- Modo de autenticación AH (Algoritmo y Claves)
- Algoritmo de cifrado ESP
- Cómo intercambiar claves
- Cada cuánto se cambian las claves
- Vida útil de la SA
- Dirección fuente de la SA

Encabezado de Autenticación (AH)

El AH, definido en IETF RFC 2402 (propuesta de norma), permite que las partes que se comunican mediante IP verifiquen que los datos no se hayan modificado durante la transmisión, y que proceden de la fuente original de la información. El AH proporciona integridad de datos sin conexión, la autenticación de los datos, y brinda protección contra ataques de repetición. El AH añade un bloque de código al paquete de datos que es el resultado de una función de “troceo” (*trash*) aplicada a todo el paquete. Hay 2 campos importantes en el encabezamiento AH:

- El índice de parámetro de seguridad (SPI) especifica al dispositivo receptor qué grupo de protocolos de seguridad está usando el emisor.
- El número de secuencia se usa para impedir ataques de repetición, al impedir el reprocesamiento múltiple de un paquete.

El campo autenticador en el AH tiene sólo 96 bits de longitud, el “emisor” ejecuta las funciones de “troceo”, trunca el número resultante para que quepa en el campo autenticador AH, y lo envía. En el otro extremo, el receptor ejecuta el mismo algoritmo de “troceo” en el paquete (como se especifica en el SPI), y trunca en consecuencia el número resultante. El receptor compara entonces el número calculado con el número del AH en el campo autenticador. Si los números corresponden al número en el paquete, se acepta como no modificado. Los dos algoritmos de “troceo” AH más usados son el resumen de mensaje 5 (*Message Digest 5: MD5*), definido por IETF RFC 2403 (propuesta de norma), que produce un autenticador de 128 bits, y el algoritmo de troceo seguro (*Secure Hashing Algorithm: SHA-1*), definido por RFC 2404 (norma), que produce un autenticador de 160 bits. El AH no mantiene los datos confidenciales y es para ocasiones cuando solamente se necesita autenticación.

Carga útil de encapsulado de seguridad (ESP)

La ESP, definida en el IETF RFC 2406, encripta la información para evitar que sea monitoreada por una entidad que no sea digna de confianza. La ESP también puede usarse para autenticación. El campo de autenticación ESP contiene la verificación de suma criptográfica que se computa sobre la parte restante de la ESP (menos el campo de autenticación ESP mismo). La autenticación AH difiere de la versión ESP en que ésta última no protege el encabezamiento IP que precede al encabezamiento ESP.

La autenticación ESP puede usarse en vez de la AH para reducir el procesamiento de paquetes, y efectúa una operación de “transformación” en vez de dos pasos. También impide los ataques de repetición siguiendo el número de la secuencia de forma muy parecida a la del AH, pero esto comprometería la validez del encabezamiento. Hay dos tipos de modo túnel y en ambos la información del encabezado original IP está encriptada; la desventaja es que no opera a través del NAT (traducción de dirección de red). En el modo transporte, el encabezado IP original no está encriptado y puede funcionar a través del NAT.

Los esquemas de encriptación ESP más usados son los siguientes:

- La norma de criptación de datos (*Data-Encryption Standard: DES*) usa una criptación de 56 bits - IETF RFC 2405 (propuesta de norma)
- La triple DES (3DES) usa una criptación de 168 bits pasando los datos a través del algoritmo DES tres veces - IETF RFC 2405 (propuesta de norma)

Gestión de Claves

Los dos métodos de uso más común para el intercambio de claves son, el primero, la codificación manual, apropiada para un número pequeño de sitios, y el segundo es mediante un protocolo definido por IETF RFC 2409, “Intercambio de claves Internet” (*Internet Key Exchange: IKE*) (propuesta de norma).

El “IKE” es una combinación de “ISAKMP” y de “Oakley”; el *Internet Security Association and Key Management Protocol* (ISAKMP), definido por IETF RFC 2408 (propuesta de norma), proporciona el marco para la autenticación y el intercambio de claves, y en el protocolo Oakley definido por el IETF RFC 2412 (informacional) se describen varios modos de intercambio de claves.

Intercambio manual de claves

El intercambio manual es la forma más fácil de gestión de claves para un número pequeño de sitios. Ambos extremos del túnel IPSec deben configurarse manualmente con las claves correspondientes. Pero la codificación manual tiene muchas desventajas:

- Es necesaria la intervención manual para actualizar o cambiar las claves.
- Como el cambio manual de claves es por lo general poco frecuente, el atacante tiene más tiempo para descifrarlas y decodificar datos.
- Hay una probabilidad de error en la configuración, dado que la misma clave debe configurarse en los dos extremos distintos del túnel IPSec.
- Si la persona con acceso a las claves se va, o deja de merecer confianza, es necesario efectuar cambios extensos de configuración.
- Las claves de la configuración deben protegerse de alguna manera contra ataques externos.

3. CONCLUSIONES

El Grupo relator sobre servicios de telefonía fija y móvil y señalización de redes recomienda la adopción de IETF RFC 2401 “Arquitectura de Seguridad para el protocolo de Internet” por parte de los Miembros y miembros asociados del CCP.I de la CITEL. Además, el grupo recomienda que RFC 2401 sea aceptado sin supresiones, adiciones o modificaciones en sus referencias normativas.

4. TRABAJO FUTURO

Durante los últimos tres años, el Grupo de Trabajo sobre Coordinación de Normas ha estado estudiando varios aspectos de las Redes de Próxima Generación, incluyendo definición de protocolos y Seguridad de Red. El Documento CCP.I/doc. 0202/03 [2] presenta una versión actualizada de estos estudios. Por lo tanto se espera que los estudios futuros en varias áreas de dicho documento den como resultado varios Documentos Coordinados de Normas.

5. DOCUMENTOS FUENTE

[1] “Arquitectura de seguridad para el protocolo de Internet”; IETF RFC 2401.

[2] “Redes de próxima Generación – Reseña de las Normas”; documento CCP.I/doc. 0202/03 (septiembre, 2003).