Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1035

(02/2007)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de las telecomunicaciones

Protocolo de intercambio de claves con autenticación mediante contraseña

Recomendación UIT-T X.1035

UIT-T

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–X.379
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.889
Aplicaciones genéricas de la notación de sintaxis abstracta uno	X.890–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LAS TELECOMUNICACIONES	**X.1000–**

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1035

Protocolo de intercambio de claves con autenticación mediante contraseña

Resumen

En la Recomendación UIT-T X.1035 se especifica un protocolo que garantiza la autenticación mutua de las dos partes que participan en el acto de establecer una clave criptográfica simétrica mediante el intercambio Diffie-Hellman. La utilización del intercambio Diffie-Hellman garantiza el *secreto perfecto en adelante*, que es, a su vez, una propiedad de un protocolo de establecimiento de claves que garantiza que una clave de sesión o una clave privada a largo plazo comprometidas después de una determinada sesión no comprometan ninguna sesión anterior. Gracias al método de autenticación propuesto el intercambio queda protegido de ataques *hombre en medio*. La autenticación se basa en un secreto precompartido (por ejemplo, una contraseña), que es protegido (es decir, se garantiza que siga sin ser revelado) contra quien escuche solapadamente, impidiéndose así un ataque de diccionario fuera de línea. Por esta razón, el protocolo puede utilizarse en aplicaciones en que los secretos precompartidos se basan en la posibilidad de que exista una contraseña débil.

Orígenes

La Recomendación UIT-T X.1035 fue aprobada el 13 de febrero de 2007 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

Aunque el intercambio *Diffie-Hellman* garantiza el *secreto perfecto en recepción*, resulta, como es bien sabido, vulnerable ante ataques *hombre en medio.* Hay varios métodos que permiten mitigar esa clase de ataque, algunos de los cuales se basan en criptografía de claves públicas, mientras que otros se basan en secretos compartidos (contraseñas). En la presente Recomendación se especifica un protocolo de este último tipo.

Concretamente, el método de autenticación propuesto permite proteger el intercambio contra ataques *hombre en medio.* La autenticación se basa en un secreto precompartido posiblemente débil, que se oculta (esto es, permanece no revelado) contra quien escuche solapadamente, lo cual impide ataques de diccionario fuera de línea. Así pues, el protocolo mencionado puede utilizarse en una amplia gama de aplicaciones en las cuales se utilizan secretos precompartidos tales como los basados en contraseñas.

Las ventajas del intercambio de claves de contraseña auténtica PAK son las siguientes:

– Permite proceder a intercambios de claves fuertes con contraseñas débiles.

– Burla los ataques hombre en medio.

– Proporciona una autenticación mutua explícita.

– Garantiza el secreto perfecto en adelante.

En los documentos que se enumeran en la bibliografía se ofrece información adicional sobre el intercambio de claves con autenticación mediante contraseña.

Recomendación UIT-T X.1035

Protocolo de intercambio de claves con autenticación mediante contraseña

1 Alcance

En esta Recomendación se da una descripción del protocolo de intercambio de claves con autenticación mediante contraseña (PAK), protocolo que atiende a los siguientes requisitos:

– Permite proceder a una autenticación mutua basándose en una clave precompartida.

– Proporciona protección contra ataques *hombre en medio* y de diccionario fuera de línea.

La Recomendación ofrece también orientación para seleccionar los parámetros del intercambio de claves Diffie-Hellman.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[TIA 683-D] TIA Standard TIA-683-D (2006), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

3 Definiciones

Ninguna.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

PAK Intercambio de claves con autenticación mediante contraseña (*password-authenticated key exchange*)

PW Contraseña (*password*)

SHA Algoritmo de troceado seguro (*secure hash algorithm*)

WLAN Red inalámbrica de área local (*wireless local area network*)

5 Convenios

En esta Recomendación se utilizan los siguientes convenios:

- *a mod b* denota último resto no negativo cuando *a* se divide por *b*.
- $H_i(u)$ denota una función de troceado convenida (por ejemplo, basada en *SHA-1*) que se computa a lo largo de una cuerda *u*, donde $i = 1, 2, 3, \ldots$ La función $H_i()$ rige con independencia de las funciones aleatorias. Se recomienda el recurso a diferentes funciones aleatorias en el protocolo PAK para fortalecer la seguridad de este protocolo.
- *s*|*t* denota la concatenación de las cuerdas *s* y *t*.

6 Descripción del protocolo

El acuerdo de clave Diffie-Hellman hace necesario que tanto el remitente como el receptor de un mensaje creen sus propios números aleatorios secretos e intercambien los exponentes de sus respectivos números. Al elevar el valor intercambiado con sus números aleatorios secretos, ambas partes pueden computar el mismo secreto compartido, clave Diffie-Hellman.

En el PAK hay dos partes que comunican, *A* y *B*, las cuales comparten una contraseña (*PW*) secreta. Se procede a seleccionar cuidadosamente las constantes globales Diffie-Hellman públicamente conocidas, un número primo *p* y un generador *g*, de tal modo que:

1) un número primo *p* seguro sea lo suficientemente largo como para hacer inviable el cómputo del logaritmo discreto; y

2) las potencias de *g* módulo *p* abarcan toda la gama de números enteros *p-1* que van de 1 a *p-1*.

En un principio, *A* selecciona un exponente secreto R_A y computa $g^{R_A} \bmod p$; *B* selecciona un exponente secreto R_B y computa $g^{R_B} \bmod p$. En aras de la eficiencia, cabe la posibilidad de utilizar exponentes cortos para R_A y R_B, siempre y cuando su tamaño no sea inferior a un determinado mínimo. En los siguientes pasos todas las operaciones de multiplicación deberían realizarse con módulo *p*, de tal modo que todos los valores que intercambian las partes que comunican no sobrepasen *p*. En consecuencia, todas las operaciones de división deberán hacerse también con mod *p*.

De ser así:

1) *A* inicia el intercambio escogiendo un R_A aleatorio y enviando a *B* la cantidad $X = H_1(A \mid B \mid PW) \cdot (g^{R_A} \bmod p)$.

2) Al recibir dicha cantidad, *B* verifica que *X* no adopte un valor nulo y procede a dividir *X* por $H_1(A \mid B \mid PW)$ para recuperar $g^{R_A} \bmod p$. A continuación, *B* elige un R_B aleatorio y computa

$$S_1 = H_3(A \mid B \mid PW \mid \frac{X}{H_1(A \mid B \mid PW)} \mid g^{R_B} \bmod p \mid \left\{\left(\frac{X}{H_1(A \mid B \mid PW)}\right)^{R_B} \bmod p\right\}) \text{ e}$$

$Y = H_2(A \mid B \mid PW) \cdot (g^{R_B} \bmod p)$. *B* envía a *A* un mensaje que contiene las cantidades S_1 e *Y*.

3) Al recibir el mensaje citado y verificar que *Y* no sea cero, *A* puede autenticar *B*, recuperando lo que debería ser $g^{R_B} \bmod p$ y computando S_1. Si el resultado es igual al valor recibido, *A* computará la clave

$$K = H_5(A \mid B \mid PW \mid g^{R_A} \bmod p \mid \frac{Y}{H_2(A \mid B \mid PW)} \mid \left\{\left(\frac{Y}{H_2(A \mid B \mid PW)}\right)^{R_A} \bmod p\right\})$$

Para autenticarse a sí mismo y completar el intercambio, *A* computa también la cantidad y la envía a *B*.

$$S_2 = H_4(A \mid B \mid PW \mid g^{R_A} \bmod p \mid \frac{Y}{H_2(A \mid B \mid PW)} \mid \left\{\left(\frac{Y}{H_2(A \mid B \mid PW)}\right)^{R_A} \bmod p\right\})$$

4) *B* autentica *A* computando S_2 y verificando el resultado sobre la base del valor recibido de *A*. Si ambos valores son idénticos, *B* computa también la clave

$$K = H_5(A \mid B \mid PW \mid \frac{X}{H_1(A \mid B \mid PW)} \mid g^{R_B} \bmod p \mid \left\{\left(\frac{X}{H_1(A \mid B \mid PW)}\right)^{R_B} \bmod p\right\}).$$

La ejecución del protocolo se detendrá si dichas verificaciones fracasan; de otro modo, ambas partes se han autentificado entre sí y establecido la correspondiente clave.

El resumen de los pasos anteriores se ilustra en la figura 1 donde *P* denota *A*|*B*|*PW* (*P = A*|*B*|*PW)* y se han simplificado algunas fórmulas.

Parte A		**Parte B**
$X = H_1(P) \cdot (g^{R_A} \bmod p)$	$\xrightarrow{X}$	Verificar que el valor recibido no sea 0 $\frac{H_1(P) \cdot (g^{R_A} \bmod p)}{H_1(P)} = g^{R_A} \bmod p$
$S_1 = H_3(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$ Calcular S_1 y verificar que es igual al valor recibido de *B* para S_1	$\xleftarrow{S_1, Y}$	$S_1 = H_3(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$ $Y = H_2(P) \cdot (g^{R_B} \bmod p)$
$S_2 = H_4(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$	$\xrightarrow{S_2}$	$S_2 = H_4(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$ Calcular S_2 y verificar que es igual al valor recibido de *A* para S_2
$K = H_5(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$		$K = H_5(P \mid g^{R_A} \bmod p \mid g^{R_B} \bmod p \mid g^{R_A R_B} \bmod p)$

Figura 1 – Descripción del protocolo PAK

7 Consideraciones de seguridad

En esta cláusula se examinan los aspectos de seguridad de PAK. Concretamente, se proporciona orientación sobre la selección de los parámetros Diffie-Hellman.

Sólo habría que utilizar en el protocolo PAK valores previamente convenidos para los parámetros *p* y *g*. Esto resulta necesario si la idea es protegerse contra un atacante que envíe valores de *p* y *g* y de este modo impulse engañosamente a la otra parte comunicante a proceder a una exponenciación Diffie-Hellman inadecuada. Utilizar los parámetros *p* y *g* de manera no conforme con los requisitos descritos en esta Recomendación puede comprometer la contraseña. En [TIA 683-D] se publican sendos valores adecuados de 1024 bits para *p* y *g*.

Asimismo, hay que señalar que si se utilizan exponentes cortos para los parámetros Diffie-Hellman R_A y R_B, estos parámetros deberían tener como mínimo un tamaño de 384 bits (suponiendo que se utilicen claves de sesión de 128 bits) y como se señala, por otra parte, en [TIA 683-D].

Las funciones aleatorias independientes H_1 y H_2 deberían arrojar cada una de ellas resultados de 1152 bits, suponiendo que el número primo *p* y las claves de la sesión K tengan respectivamente por longitud 1024 bits y 128 bits. Las funciones aleatorias H_3, H_4 y H_5 deberían arrojar un resultado de 128 bits.

EJEMPLO: Cabría la posibilidad de recomendar la utilización de las funciones de troceado [b-FIPS 180-2] SHA-1 para la ejemplificación de las funciones aleatorias $H_i()$ descritas en [b-TIA 1050]. Con todo, habría que señalar que el NIST se encuentra alentando la utilización de SHA-256 como una opción más segura que SHA-1.

Bibliografía

[b-TIA 1050] TIA 1050-100, Project Number 3-0174-000, *Wireless Local Area Network (WLAN) Interworking*.

[b-FIPS 180-2] NIST Federal Information Processing Standards, Publication FIPS 180-2 (2002), *Secure Hash Standard*.

[b-EUROCRYPT] BOYKO (V.), MACKENZIE (P.), PATEL (S.): Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman, EUROCRYPT 2000.

[b-IEEE P1363.2] IEEE P1363.2 (Sept. 2006), *Standard Specifications for Password-Based Public-Key Cryptographic Techniques*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2007