Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1210

(01/2014)

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

Seguridad en el ciberespacio – Ciberseguridad

Aspectos generales de los mecanismos de detección del origen de los problemas de seguridad en las redes de protocolo Internet

Recomendación UIT-T X.1210

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
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	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339

Recomendación UIT-T X.1210

Aspectos generales de los mecanismos de detección del origen de los problemas de seguridad en las redes de protocolo Internet

Resumen

En la Recomendación UIT-T X.1210 se presentan los mecanismos de detección del origen de los problemas de seguridad, además de los criterios de selección y las directrices de seguridad básica de esos mecanismos.

Para detectar el origen de los problemas de seguridad en las redes de protocolo Internet se emplean técnicas para obtener información técnica sobre los puntos de ingreso, los trayectos, los trayectos parciales u orígenes de un paquete o paquetes que causan problemas en la red, normalmente con el objetivo de solucionarlos.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1210	2014-01-24	17	11.1002/1000/12043

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) 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

Recomendación UIT-T X.1210

Aspectos generales de los mecanismos de detección del origen de los problemas de seguridad en las redes de protocolo Internet

1 Alcance

En esta Recomendación se presentan los aspectos generales de los mecanismos de detección del origen de los problemas de seguridad, los criterios de evaluación y las directrices de seguridad básica de esos mecanismos.

Los implementadores y usuarios de la presente Recomendación del UIT-T deberán ajustarse a las leyes, reglamentos y políticas nacionales y regionales aplicables.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 denegación de servicio [b-UIT X.800]: Prevención de acceso autorizado a recursos o retardo deliberado de operaciones críticas desde el punto de vista del tiempo.

3.1.2 dominio de seguridad [b-UIT-T T.411]: Conjunto de recursos sometidos a una única política de seguridad.

3.1.3 amenaza [b-UIT-T X.800]: Violación potencial de la seguridad.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

AS	Sistema autónomo (*autonomous system*)
BGP	Protocolo de pasarela de frontera (*border gateway protocol*)
DoS	Denegación de servicio (*denial of service*)
ICMP	Protocolo de mensaje de control Internet (*internet control message protocol*)
IP	Protocolo Internet (*Internet protocol*)
IPFIX	Exportación de información de flujo IP (*IP flow information export*)
IPv4/v6	Protocolo Internet versión 4/versión 6 (*Internet protocol version 4/version 6*)
PSI	Proveedor de servicio Internet
RID	Defensa entre redes en tiempo real (*real-time inter-network defence*)
TCP	protocolo de control de transmisión (*transmission control protocol*)

5 Convenios

Ninguno.

6 Generalidades de los mecanismos de detección del origen de los problemas de seguridad

La detección del origen de los problemas de seguridad en las redes de protocolo Internet (IP) suele conllevar un proceso técnico y/o administrativo destinado a identificar de manera fiable el origen de un paquete o paquetes IP cuya dirección IP del emisor se ha introducido correcta o incorrectamente, o cuyo trayecto, o partes del mismo, pueden causar problemas de seguridad.

Los mecanismos de detección del origen de los problemas de seguridad pueden emplearse para identificar la ubicación física o lógica de tales incidentes de seguridad en tiempo real gracias a la ayuda de elementos de la red, como los encaminadores o anfitriones.

A continuación se exponen los mecanismos de detección de los problemas de seguridad en las redes IP.

6.1 Detección del origen de los problemas de seguridad con prueba de enlace

La detección de los problemas puede empezarse por el encaminador más próximo a la víctima y probar su enlace ascendente hasta que los proveedores de servicio Internet puedan determinar cuál de ellos se está utilizando para transportar el tráfico perjudicial. En condiciones ideales, este procedimiento se repite en los encaminadores en sentido ascendente hasta identificar el origen del problema de seguridad.

Esta técnica asume que el problema de seguridad permanece activo hasta que se finaliza el procedimiento de detección, por lo que no resulta adecuada para ataques que se detectan después de su ejecución, para los ataques intermitentes o los ataques que modulan su comportamiento en función de la detección de problemas de seguridad.

La depuración de la entrada es una de las aplicaciones del mecanismo de prueba de enlace. Se trata de una función ya existente en muchos encaminadores, que permite al administrador detectar los enlaces de red entrantes de paquetes concretos. Si el operador del encaminador conoce las características específicas del tráfico de ataque (lo que se denomina "firma del ataque"), puede determinar el enlace de red entrante en el encaminador.

6.2 Detección del origen de los problemas de seguridad con red superpuesta

El aislamiento [b-IETF RFC 3882] es una técnica operativa mediante la cual se implanta un túnel en todos los puntos por los que un ataque puede llegar al sistema autónomo (AS) víctima/de destino. Utilizando un protocolo de pasarela de frontera (BGP) [b-IETF RFC 4271], es posible aislar el tráfico destinado al anfitrión víctima/objetivo, es decir, descartarlo de la red o reencaminarlo por un trayecto especial (túnel) donde un dispositivo puede capturarlo para analizarlo y, posteriormente, descartarlo.

6.3 Detección del origen de los problemas de seguridad con sondas

El protocolo de mensaje de control Internet (ICMP) para la versión 4 del protocolo Internet (IPv4) [b-IETF RFC 792] y la versión 6 del protocolo Internet (IPv6) [b-IETF RFC 4443], han sido y seguirán siendo uno de los mecanismos de detección de problemas en redes IP más útiles. Hay una serie de herramientas, como ping y traceroute, que están incorporadas en los sistemas operativos comunes que emplean ICMP para efectuar una detección de problemas de extremo a extremo o a nivel de enlace.

6.4 Detección del origen de los problemas de seguridad con registro y muestreo

El muestreo de flujo puede ser útil como mecanismo de detección de problemas de seguridad en las redes IP. Los operadores pueden emplear sFlow [b-IETF RFC 3176], NetFlow [b-IETF RFC 3954], o la exportación de información de flujo IP (IPFIX) [b-IETF RFC 5655] habida cuenta de las normas de muestreo de flujo que soporten los encaminadores existentes.

6.5 Detección del origen de los problemas de seguridad en sistemas autónomos

En caso de problemas de seguridad a gran escala a lo largo de sistemas autónomos, los operadores pueden confiar en las herramientas de detección de problemas basadas en las sondas (véase la cláusula 6.3) y en las sondas en línea disponibles en Internet, por ejemplo, Looking Glass [b-LG]. En el futuro, los operadores podrán facilitar el intercambio de información entre herramientas de detección de problemas más avanzadas en sistemas autónomos, por ejemplo, empleando la defensa entre redes en tiempo real (RID) [b-IETF RFC 6045].

7 Directrices de seguridad básicas de los mecanismos de detección del origen de los problemas de seguridad

Las directrices de seguridad básicas de los mecanismos de detección del origen de los problemas de seguridad se presentan a continuación:

- Los mecanismos de detección del origen de los problemas de seguridad deben diseñarse de manera que sean adaptables, robustos y resistentes.
- Los mecanismos de detección del origen de los problemas de seguridad deben implantarse y ejecutarse en múltiples dominios, cada uno de los cuales estará gestionado por un administrador de seguridad responsable (es decir, detección de problemas entre sistemas autónomos).
- Los mecanismos de detección del origen de los problemas de seguridad deben aplicarse siguiendo uno de los dos modelos de implantación: centralizado o distribuido.
- Los mecanismos de detección del origen de los problemas de seguridad deben ofrecer técnicas para obtener información técnica sobre los puntos de ingreso, los trayectos, los trayectos parciales u orígenes de un paquete o paquetes que causan problemas en la red, normalmente con el objetivo de solucionarlos.
- A fin de seleccionar un mecanismo adecuado de detección del origen de los problemas de seguridad, han de evaluarse los mecanismos en función de los criterios indicados en la cláusula 8.
- La interfaz de los mecanismos de detección del origen de los problemas de seguridad en sistemas autónomos ha de garantizar la confidencialidad, la autentificación del origen de los datos y la integridad de la información intercambiada entre los diversos dominios de seguridad, y puede asegurar la disponibilidad del mecanismo de detección de problemas.

8 Criterios para evaluar los mecanismos de detección del origen de problemas

Los criterios que se han de utilizar para evaluar los mecanismos de detección de problemas se especifican a continuación:

- Grado de participación del proveedor de servicio Internet (PSI): grado de participación del PSI cuando un administrador PSI especifica la detección de problemas. La mayoría de mecanismos de detección de problemas asumen que el PSI facilita parte de sus instalaciones para efectuar la detección de problemas. Un programa de detección de problemas ideal exige un bajo nivel de participación del PSI.

- Número de paquetes necesario para la detección de problemas: número de paquetes utilizados por el administrador necesario para identificar el origen del problema de seguridad una vez constatado el mismo.
- Eficacia de la aplicación parcial: grado de eficacia de la detección de problemas cuando se realiza de manera parcial con un único PSI. La eficacia oscila entre la incapacidad de identificación y la identificación significativa.
- Tara de procesamiento para la detección de problemas: cantidad de procesamiento extra que ha de realizar el elemento de red intermedio o el posible anfitrión víctima. Se preferirá un plan de detección de problemas que exija un mínimo de procesamiento extra para el elemento de red intermedio o el anfitrión víctima.
- Grado de aumento del ancho de banda: cantidad adicional de tráfico necesario para la detección de problemas. Un mecanismo de detección de problemas más conveniente necesitará una cantidad mínima o nula de ancho de banda adicional.
- Requisitos de memoria: cantidad de memoria adicional que necesitan los elementos de red o el servidor de detección de problemas dedicado. No es conveniente que se exija más memoria al elemento de red, mientras que sí se puede tolerar en el caso de los servidores dedicados. Un mecanismo de detección de problemas ideal exigirá una cantidad limitada de memoria adicional en el servidor dedicado, pero no en el elemento de red.
- Robustez de la detección de problemas: capacidad del mecanismo de detección de problemas para ofrecer resultados significativos, incluso si algunos elementos de red que participan en el proceso se han trastornado. El trastorno se debe a errores derivados de la configuración errónea del elemento de red o de un parche de software inadecuado.
- Adaptabilidad: cantidad de configuración adicional que se ha de realizar en los demás elementos de red para añadir un único elemento de red nuevo. Esto indica con cuánta facilidad puede ampliarse el programa de detección de problemas. Se considera que la adaptabilidad es buena si sólo se ha de configurar el elemento de red añadido, y se considera que es mediocre si la adición de un único elemento de red exige la configuración completa del resto de elementos de red. Un mecanismo de detección de problemas ideal debe ser adaptable.
- Número de funciones necesarias para efectuar la detección de problemas: cantidad de funciones adicionales necesarias para aplicar un programa de detección de problemas dado.
- Capacidad de manejo de problemas de seguridad masivos en toda la red: capacidad del programa de detección de problemas para reflejar en qué medida puede identificar problemas de seguridad en toda la red. Un programa de detección de problemas ideal ha de poder identificar cualquier problema de seguridad, incluidos los ataques de denegación de servicio distribuido DDoS.
- Capacidad para detectar problemas en paquetes transformados: capacidad del programa de detección de problemas para identificar el origen de los problemas incluso cuando se han transformado los paquetes. Por transformación de paquetes se entiende su modificación al efectuar un reenvío de paquetes. Una transformación común es la traducción de dirección, proceso durante el cual se modifica(n) la(s) dirección(es) de origen y/o destino del(de los) paquete(s).

Bibliografía

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[b-UIT-T T.411] Recomendación UIT-T T.411 (1993), *Tecnología de la información – Arquitectura de documento abierta y formato de intercambio: Introducción y principios generales*.

[b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[b-IETF RFC 3176] IETF RFC 3176 (2001), *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

[b-IETF RFC 3882] IETF RFC 3882 (2004), *Configuring BGP to Block Denial-of-Service Attacks*.

[b-IETF RFC 3954] IETF RFC 3954 (2004), *Cisco Systems NetFlow Services Export Version 9*.

[b-IETF RFC 4271] IETF RFC 4271 (2006), *A Border Gateway Protocol 4 (BGP-4)*.

[b-IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

[b-IETF RFC 5655] IETF RFC 5655 (2009), *Specification of the IP Flow Information Export (IPFIX) File Format*.

[b-IETF RFC 6045] IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID)*.

[b-LG] BGP Looking Glass, http://www.lookinglass.org/.

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	Terminales y métodos de evaluación subjetivos y objetivos
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, 2015