Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1253

(09/2011)

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

Seguridad en el ciberespacio – Gestión de identidades

Directrices de seguridad para los sistemas de gestión de identidades

Recomendación UIT-T X.1253

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
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589

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

Recomendación UIT-T X.1253

Directrices de seguridad para los sistemas de gestión de identidades

Resumen

En la Recomendación UIT-T X.1253 se proponen directrices de seguridad para los sistemas de gestión de identidades (IdM). Las directrices de seguridad indican cómo deben instalarse y utilizarse los sistemas IdM para ofrecer servicios de identidad seguros en las NGN (red de la próxima generación) o en el ciberespacio. Las directrices de seguridad consisten en consejos oficiales sobre cómo utilizar los diversos mecanismos de seguridad para proteger los sistemas IdM generales y, además, proporciona los procedimientos de seguridad adecuados para el interfuncionamiento de los sistemas IdM.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1253	2011-09-02	17

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.1253

Directrices de seguridad para los sistemas de gestión de identidades

1 Alcance

El ámbito de aplicación de la presente Recomendación es el siguiente:

– modelos y servicios de sistemas IdM generales;

– amenazas y riesgos de seguridad relacionados con los sistemas IdM;

– directrices de seguridad para la instalación de sistemas IdM;

– directrices de seguridad para la utilización de sistemas IdM;

– consideraciones relativas a la privacidad en sistemas IdM.

La presente Recomendación se ha concebido principalmente para servicios de gestión de identidades basados en múltiples dominios. Ahora bien, estas directrices también pueden aplicarse a sistemas de gestión de identidades centralizados.

NOTA – Al aplicar y utilizar estas directrices se habrá de cumplir la legislación, la normativa y las políticas nacionales y regionales aplicables. Cierta reglamentación y legislación específicas podrían requerir la aplicación de mecanismos para proteger la información personal.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios a que estudien la posibilidad de utilizar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente en vigor. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación

[UIT-T X.1205] Recomendación UIT-T X.1205 (2008), *Aspectos generales de la ciberseguridad*.

[UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones de referencia para la gestión de la identidad*.

3 Términos y definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 control de acceso [UIT-T X.1252]: Procedimiento utilizado para determinar si se debe conceder a una entidad acceso a recursos, instalaciones, servicios o informaciones, en función de las normas preestablecidas y la autoridad o los derechos específicos de la parte solicitante.

3.1.2 atributo [UIT-T X.1252]: Información relacionada con una entidad que especifica una característica de la entidad.

3.1.3 autentificación (de entidad) [UIT-T X.1252]: Proceso utilizado para obtener un nivel de confianza suficiente en la vinculación entre la entidad y la identidad presentada.

3.1.4 credencial [UIT-T X.1252]: Conjunto de datos presentado como evidencia de una identidad y/o unos derechos declarados.

3.1.5 identidad [UIT-T X.1252]: Representación de una entidad bajo la forma de uno o varios atributos que permiten distinguir suficientemente a la entidad o entidades dentro del contexto. A los efectos de la gestión de identidad (IdM), se entiende que este término constituye una identidad contextual (subconjunto de atributos), es decir que la diversidad de atributos está limitada por un marco con fronteras definidas (el contexto) en el cual existe e interactúa la entidad.

NOTA – Cada entidad está representada por una identidad holística, que comprende todos los posibles elementos de información que caracterizan a dicha entidad (los atributos). Sin embargo, la identidad holística es una cuestión teórica y elude cualquier descripción y utilización práctica, dado que el número de todos los atributos posibles es indefinido.

3.1.6 gestión de identidad (IdM) [UIT-T X.1252]: Conjunto de funciones y capacidades (por ejemplo, administración, gestión y mantenimiento, descubrimiento, intercambios de comunicación, correlación y vinculación, cumplimiento de una política, autentificación y asertos) que se utilizan para:

- garantizar la información de identidad (por ejemplo, identificadores, credenciales, atributos);
- garantizar la identidad de una entidad (por ejemplo, usuarios/abonados, grupos, dispositivos de usuario, organizaciones, proveedores de red y de servicios, elementos y objetos de red, objetos virtuales); y
- aplicaciones comerciales y de seguridad.

3.1.7 usuario [UIT-T X.1252]: Entidad que utiliza un recurso, por ejemplo sistemas, equipos, terminales, procesos, aplicaciones o redes empresariales.

3.1.8 centrado en el usuario [UIT-T X.1252]: Un sistema de gestión de identidad (IdM) que puede proporcionar al usuario la capacidad de controlar y hacer cumplir diversas políticas de privacidad y seguridad que rigen el intercambio de información sobre identidad, en particular la información de identificación personal del usuario.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos

3.2.1 entidad: Cualquier cosa que tenga una existencia autónoma y bien definida y pueda ser identificada en contexto.

NOTA – Una entidad puede ser una persona física, un animal, una persona jurídica, una organización, una cosa activa o pasiva, un dispositivo, una aplicación informática, un servicio, etc., o un grupo de estos elementos. En el contexto de las telecomunicaciones, como ejemplos de entidades cabe mencionar puntos de acceso, abonados, usuarios, elementos de red, redes, aplicaciones informáticas, servicios y dispositivos, interfaces, etc.

3.2.2 cliente IdM: Programa cliente que interactúa con el servidor IdM para obtener información sobre la identidad.

3.2.3 servidor IdM: Servidor que gestiona el ciclo de vida de la identidad de un usuario.

3.2.4 cliente IdM móvil: Cliente IdM que se instala y utiliza en un dispositivo móvil.

4 Siglas y acrónimos

En esta Recomendación se utilizan las siguientes siglas y acrónimos:

DB Base de datos (*database*)

DoS Denegación del servicio (*denial of service*)

FDDI Interfaz de datos distribuidos por fibra (*fibre distributed data interface*)

IdM Gestión de identidad (*identity management*)

IdP Proveedor de identidad (*identity provider*)

IDS Sistema de detección de intrusión (*intrusion detection system*)

IPS Sistema de prevención de intrusión (*intrusion prevention system*)

LAN Red de área local (*local area network*)

NGN Red de la próxima generación (*next generation network*)

OS Sistema operativo (*operating system*)

PII Información identificable personalmente (*personally identifiable information*)

PIN Número de identificación personal (*personal identification number*)

PKI Infraestructura de claves públicas (*public key infrastructure*)

SP Proveedor de servicio (*service provider*)

SSL Capa de conexión segura (*secure socket layer*)

TTP Tercero fiable (*trusted third party*)

VPN Red privada virtual (*virtual private network*)

5 Convenios

Ninguno.

6 Antecedentes

En la última década, los sistemas de gestión de identidad (IdM) han evolucionado desde un sistema silo a un sistema IdM federado o centrado en el usuario. La mayoría de los sistemas IdM desarrollados hasta la fecha se concentran en cómo ofrecer los servicios relacionados con la identidad de la manera más eficaz y conveniente. Muchos de los sistemas IdM desarrollados recientemente tratan de proporcionar seguridad y privacidad.

Al principio los sistemas IdM conocidos como el modelo silo se instalaban en el dominio de la empresa. Como cada sistema IdM no estaba conectado en modo alguno con los demás, resultaba imposible compartir información sobre la identidad del usuario para proporcionar servicios útiles entre dominios. Además, la identidad de un mismo usuario podría duplicarse en diferentes sistemas IdM, por lo que la gestión eficaz y segura de la identidad del usuario resultaba difícil para la administración del sistema de una organización.

La siguiente fase consistió en recabar todas las identidades del usuario en un solo sistema IdM y distribuirla cuando era necesario. Este método se denominó modelo centralizado. En este modelo se reúne demasiada información sobre un usuario en un mismo servidor. El modelo presenta varios inconvenientes, por cuanto el proveedor de identidad se convierte en un punto débil y, además, quizá no todas partes confíen en dicho proveedor.

El método que pasó a utilizarse a continuación consistía en dejar que cada proveedor de identidad gestionara su propia identidad y descentralizar su responsabilidad, de modo que cada usuario pueda elegir entre varios de estos proveedores. Este modelo se conoce como el modelo federado. En este modelo existen múltiples proveedores de identidad en los que puede confiar un usuario y que gestionan, si procede, una parte de la información sobre la identidad. Para compartir la información sobre la identidad del usuario en cada proveedor de identidad se recurre a una parte de un seudónimo denominado identidad federada. Con este modelo se evita el problema de que el proveedor sea un punto débil.

A medida que las cuestiones relativas a la privacidad del usuario adquieren cada vez mayor importancia, la tecnología IdM ha derivado en conceder al usuario el pleno control de su información de identidad. Este paradigma se conoce como modelo centrado en el usuario. En este modelo, la información de identidad debe pasar a través del usuario para que éste tenga la oportunidad de aplicar su propia política de privacidad cuando dos proveedores de identidad comparten información sobre la identidad del usuario. Muchos productos industriales se han adaptado a este modelo, que integra otras tecnologías IdM existentes.

La convergencia de estos sistemas IdM plantea a menudo la dificultad de cómo garantizar la seguridad del sistema convergente y de cómo llegar a un equilibrio entre la seguridad y la privacidad para ofrecer un rendimiento óptimo. Por otra parte, la mayoría de las directrices de seguridad proporcionadas hasta la fecha consisten en un proveedor de identidad y en partes que confían en el mismo. Cuando los aspectos relacionados con la seguridad y privacidad del usuario se convierten en un requisito obligatorio, resulta imprescindible considerar la parte centrada en el usuario de la seguridad de los sistemas IdM para tomar en consideración la creciente preocupación acerca de la privacidad del usuario.

7 Descripción general de los sistemas de gestión de identidad

7.1 Modelo general de los sistemas IdM

7.1.1 Sistema IdM centrado en la aplicación

En los sistemas IdM de gran escala, por sistema IdM centrado en la aplicación se entiende que los servicios y las políticas de identidad se han concebido para satisfacer los requisitos de los proveedores de identidad y de las partes que confían en éste, y que se han optimizado para las necesidades de las aplicaciones, por ejemplo, para la configuración de la información sobre la cuenta del usuario. En los sistemas IdM centrados en la aplicación existe un proveedor de identidad y una parte que confía en el mismo. Cuando se presta un servicio de identidad al usuario, lo normal es que estas dos entidades efectúen un intercambio de identidad. Anteriormente, las tecnologías de gestión del acceso y de identidad consistían principalmente en la autentificación de los usuarios para obtener acceso federado a aplicaciones y servicios. Por consiguiente, el requisito de seguridad se limita al perímetro de su dominio de aplicación.

7.1.2 Sistemas IdM centrados en el usuario

Los sistemas IdM centrados en el usuario se concentran principalmente en los usuarios finales y están optimizados para satisfacer sus necesidades. Esto significa que el principal objetivo de un sistema IdM es proporcionar servicios de identidad convenientes y completos a los usuarios. Su principal característica reside en que dan al usuario pleno control sobre su identidad. Cuando se divulga información sobre la identidad del usuario, ésta debe pasar explícitamente a través del usuario para que éste tenga la oportunidad de aplicar, si lo estima necesario, políticas personales. En los sistemas IdM centrados en el usuario, tiene que instalarse un programa cliente en el entorno informático del usuario. Por consiguiente, se requieren directrices de seguridad fáciles y detalladas que ayuden al usuario a instalar y utilizar de manera segura el software correspondiente. Este software debe gestionar cierta información relacionada con la seguridad del usuario.

Los sistemas centrados en el usuario se diferencian de otros modelos de IdM en que es el propio usuario, y no una autoridad, quien mantiene el control sobre cómo se crean, distribuyen, actualizan y anulan atributos sobre su identidad. Esto significa que el usuario tiene plena autoridad de su identidad a lo largo del ciclo de vida de ésta. El nivel de control puede determinarse mediante los requisitos de privacidad del usuario.

7.2 Servicios de identidad

7.2.1 Gestión del ciclo de vida de identidad

Se trata del servicio que gestiona la creación, liberación, actualización y anulación de la identidad. Los datos relacionados con este servicio se almacenan en una base de datos ubicada en un servidor o en una máquina local. Por consiguiente, el acceso a esta base de datos debe estar restringido exclusivamente a los usuarios autorizados.

7.2.2 Autentificación

Un servicio de autentificación verifica la legitimidad de las entidades o los usuarios que solicitan acceso al sistema o a los recursos. La autentificación es el servicio fundamental que ofrece el sistema IdM a las partes que confían. Debe impedirse a toda costa la falsificación o el pirateo de las contraseñas.

7.2.3 Autorización

Un servicio de autorización está concebido para tomar decisiones en materia de derechos de acceso del usuario y aplicar las decisiones de autorización con arreglo a los privilegios del usuario. Este servicio es imprescindible para proteger el sistema de identidad contra utilización y acceso no autorizados.

7.2.4 Intercambio de atributos

Este servicio se encarga del intercambio y la sincronización de atributos. Es uno de los servicios más esenciales en lo que respecta a la seguridad, dado que los atributos se intercambian por redes de comunicaciones. Se requieren diferentes mecanismos de seguridad en función de si el medio de comunicación es alámbrico o inalámbrico.

7.2.5 Testigos de seguridad

Un servicio de testigos de seguridad es necesario para que las entidades puedan compartir información sobre seguridad o identidad. Por lo general, los testigos de seguridad están protegidos mediante mecanismos de seguridad o criptográficos dado que siempre contienen información muy confidencial que no debe hacerse pública.

8 Amenazas de seguridad en sistemas IdM

Se supone que la mayoría de las amenazas de seguridad que existe en el ciberespacio también existen en los sistemas IdM, dado que éstos funcionan en el ciberespacio. Las amenazas generales a la seguridad en el ciberespacio se describen en la [UIT-T X.1205].

En los sistemas IdM existen diversas amenazas de seguridad que lo hacen vulnerable o ponen en grave peligro a la organización.

8.1 Seguridad en los sistemas

En general, la seguridad en los sistemas se refiere a la protección de los equipos y los datos del usuario. La finalidad es que sólo puedan acceder a los equipos los usuarios autorizados y para la finalidad prevista por los propietarios. Además, el sistema sólo deberá utilizarse para tales fines. Los agresores no deben poder eliminar la legitimidad de los usuarios de recursos.

8.1.1 Utilización y acceso no autorizados

La mayoría de los sistemas no deben permitir el acceso y la utilización por parte de usuarios no autorizados. Los sistemas IdM deben ser muy rigurosos a la hora de impedir que exista este tipo de vulnerabilidad de la seguridad, por cuanto el acceso no autorizado a identidades en un sistema IdM puede originar otras amenazas a la seguridad, tales como el robo y la suplantación de identidad.

8.1.2 Utilización indebida

Por utilización indebida se entiende la utilización del sistema IdM para procesar o llevar a cabo una tarea que no estaba prevista en un principio. Los usuarios autorizados deben tener ciertas limitaciones a la hora de utilizar partes del sistema IdM sin privilegios adecuados. Algunos servicios están restringidos para usuarios autorizados, otros para usuarios específicos y algunos servicios suelen estar prohibidos en general salvo para los administradores.

8.1.3 Denegación del servicio

Por lo general el sistema IdM es la puerta de entrada del usuario antes de utilizar los servicios de aplicación. Por consiguiente es muy probable que los sistemas IdM sean objeto de ataques destinados a interrumpir la prestación de servicios. Son posibles muy diversos ataques a los sistemas IdM para llevar a cabo una denegación del servicio. Este tipo de ataques son muy fáciles de ejecutar y muy difíciles de contrarrestar. Muchos de estos ataques están pensados para consumir enormes recursos informáticos, lo que dificulta o imposibilita la prestación de servicio a los usuarios legítimos.

8.2 Amenazas a la seguridad pasivas

Las amenazas a la seguridad pasivas consisten en que el agresor lee los paquetes que circulan por la red pero no los modifica. La forma más fácil de llevar a cabo este tipo de ataque es sencillamente estar conectado a la misma LAN que la víctima. En las configuraciones las más comunes, en particular Ethernet, 802.3 y FDDI, cualquier máquina conectada por cable puede leer todo el tráfico destinado a cualquier otra máquina situada en la misma LAN.

Los canales de comunicación inalámbricos requieren consideración especial, sobre todo por el auge de la popularidad que están teniendo recientemente las LAN inalámbricas, tales como las que utiliza 802.11. Dado que los datos se retransmiten en frecuencia radioeléctricas bien conocidas, el agresor sólo necesita ser capaz de recibir dichas transmisiones. Esos canales son especialmente vulnerables a los ataques pasivos. Aunque muchos de estos canales cuentan con protección criptográfica, suele suceder que esta tecnología de seguridad se emplea sin estar correctamente configurada.

8.2.1 Quebranto de la confidencialidad

El ataque a la confidencialidad consiste en intervenir cualquier conversación o comunicación privada que se lleva a cabo en la línea de comunicación. En Internet siguen habiendo muchos casos en los que la información confidencial se transmite sin protección alguna. Toda credencial que se obtiene mediante este ataque puede reutilizarse para ataques ulteriores.

8.2.2 Averiguación de contraseñas

La averiguación de contraseñas consiste en recabar contraseñas de usuario que se transmiten por la red con el fin de obtener acceso no autorizado a los recursos. El agresor que puede leer este tráfico es capaz luego de averiguar la contraseña y reproducirla. Es decir, el agresor puede iniciar una conexión con el sistema IdM para robar información sobre la identidad del usuario.

8.3 Amenazas a la seguridad activas

Por ataque activo se entiende un ataque en el que se modifican los datos en la red o en el sistema. Los ataques activos son una intrusión en una red informática con el objetivo de suprimir o modificar los datos almacenados en los sistemas IdM que forman parte de la red. Se trata de una de las formas de ataque más graves dado que el funcionamiento de muchas empresas depende sobremanera en los datos.

8.3.1 Ataques por reproducción

Este tipo de ataque consiste en que el agresor graba una secuencia de mensajes que circulan por el cable y luego la reproduce a la parte correspondiente que los recibió originalmente. Obsérvese que el/la agresor/a no necesita comprender los mensajes, sino que se limita a capturarlos y retrasmitirlos.

8.3.2 Ataque por intromisión

El agresor socava el flujo de comunicación con el fin de situarse como remitente para el receptor y como receptor para remitente. Este tipo de ataque es muy grave dado que suplanta tanto al remitente como al receptor. Por consiguiente, muchas técnicas que controlan la integridad del flujo de comunicación son insuficientes para protegerse contra los ataques por intromisión. Este tipo de ataques puede realizarse siempre que el protocolo carezca de autentificación de entidades pares.

8.4 Amenazas a la seguridad relacionadas con los sistemas IdM

Se trata de las amenazas que están especialmente relacionadas con los sistemas IdM. Las amenazas que se indican a continuación constituyen los principales puntos débiles de la seguridad, por las cuales todo sistema IdM debe tomar las medidas necesarias para contrarrestarlos.

8.4.1 Amenazas relacionadas con las contraseñas

Una de las amenazas relacionadas con la contraseña se debe a que ésta es débil. Si el usuario elige una contraseña de autentificación débil, es decir, fácil de adivinar, la contraseña puede obtenerse mediante un ataque por diccionario. Otro problema se produce cuando el usuario utiliza una y otra vez la misma contraseña débil para diversos sitios web. En este caso, el agresor puede efectuar un ataque a un sitio que tenga un fallo de seguridad para obtener la contraseña del usuario y luego sólo tiene que probar a entrar en otro sitio web utilizando la contraseña robada en el primero.

La otra amenaza consiste en averiguar la contraseña mediante software espía (*spyware*) instalado en un computador. Cualquier computador puede resultar infectado por software espía cuya función es piratear la contraseña del usuario o del administrador.

8.4.2 Acceso no autorizado

El acceso no autorizado es un término que puede referirse a toda una serie de ataques. La meta final del agresor es acceder ilegalmente a recursos [UIT-T X.1205].

Un sistema IdM que ofrece servicios de autentificación y de identidad tiene que estar disponible y ser accesible por todas las partes que necesitan conocer la identidad del usuario para prestar servicios de aplicación. Por consiguiente, se requiere de un mecanismo de control de acceso bastante preciso para proteger al sistema contra los accesos no autorizados.

8.4.3 Escucha

La escucha es una amenaza difícil de detectar. El objetivo del agresor es escuchar y, sobre todo, registrar datos brutos que circulan por la LAN de la empresa. Este ataque utiliza un "modo promiscuo" de los adaptadores en Internet que se encuentran en el mercado. Este modo permite al agresor capturar todos los paquetes de la red. Hay muchos rastreadores de red gratuitos en la vuelta que los agresores pueden emplear para efectuar escuchas [UIT-T X.1205].

Los sistemas IdM suelen comunicarse con usuarios y otras entidades, a través de redes alámbricas o inalámbricas para compartir credenciales e información sobre identidades, que suele ser confidencial. Por consiguiente, toda información que reciba la persona que tiene intervenida la comunicación puede causar el robo de identidad.

8.4.4 Peska (*phishing*)

Consiste en el intento por un tercero de solicitar información confidencial a un individuo, grupo u organización mimetizando o falsificando una determinada marca, por lo general muy conocida, normalmente con el fin de obtener un beneficio económico. El agresor trata de engañar a los usuarios para que revelen datos personales, tales como números de tarjeta de crédito, credenciales de los servicios bancarios en línea, y otra información sensible que luego pueden utilizar para cometer actos fraudulentos. Un sitio web de peska es un sitio diseñado para mimetizar un sitio web legítimo de una organización cuya marca se está falsificando. En los sistemas IdM, la peska se considera una amenaza grave dado que puede utilizarse la información de autentificación de la víctima u otra información personal para probar la identidad o llevar a cabo una actividad fraudulenta una vez que el agresor haya obtenido esa información.

8.4.5 Robo de identidad

Se trata de un problema de seguridad muy grave, especialmente para organizaciones que almacenan y gestionan grandes cantidades de información de identidad personal. Además de poner en peligro la pérdida de datos personales y menoscabar la confianza entre el cliente y la institución, así como causar daños importantes a la reputación de la organización, la violación de datos también puede tener repercusiones financieras para las organizaciones.

9 Directrices de seguridad para los sistemas IdM

Las directrices de seguridad que figuran en las cláusulas 9.1 y 9.2 especifican cómo gestionar la seguridad al instalar y utilizar sistemas IdM generales. Estas directrices indican prescripciones de seguridad básicas de los sistemas IdM que pueden instalarse y utilizarse con seguridad en diversos entornos informáticos. Las cláusulas 9.3, 9.4 y 9.5 tratan de las entidades del sistema IdM, a saber, el servidor, el cliente y el cliente móvil IdM. En la cláusula 9.6 se describen consideraciones relativas a la privacidad en los sistemas IdM.

9.1 Directrices de seguridad para la instalación de sistemas IdM

En esta cláusula figuran las directrices de seguridad para la instalación y despliegue de sistemas IdM. En la mayoría de los casos, la dificultad radicará en la preparación de la gestión de la confianza y de claves.

9.1.1 Gestión de la confianza

Toda autorización que se efectúa utilizando sistemas IdM depende de la confianza en que la identidad y su atributo sean auténticos y correctos. Por consiguiente, una identidad sólo resulta útil cuando ha sido autorizada. La autoridad se basa en la confianza. Así pues, el plan de gestión de confianza constituye la primera etapa para instalar y utilizar satisfactoriamente un sistema IdM.

La infraestructura de clave pública (PKI, *public key infraestructura*) es uno de los mecanismos de confianza fundamentales para el sistema de gestión de identidad. La principal finalidad de la PKI es proporcionar un certificado de clave pública que pueda utilizarse para autentificar y proteger el canal. En el caso de sistemas IdM de gran escala, se recomienda encarecidamente crear un TTP (tercero de confianza – *trusted third party*) utilizando la PKI. El certificado que expide la PKI puede utilizarse para autentificar los usuarios en el sistema IdM y encriptar el canal de comunicación en SSL. Otra aplicación fundamental de los certificados es la firma digital.

9.1.2 Seguridad en la red

Es fundamental proteger el entorno de red de diversas maneras. En primer lugar, el perímetro de la red debe protegerse mediante un cortafuegos. Todo sistema IdM debe residir dentro del perímetro del cortafuegos. Además, pueden emplearse mecanismos de seguridad de red más sofisticados tales como VPN y IDS/IPS para lograr un entorno de red más seguro.

9.1.3 Entorno de alojamiento seguro

El entorno de alojamiento es donde se instalan y funcionan los sistemas IdM. Es indispensable que los servidores y estaciones de trabajo donde se vaya a instalar el componente del sistema IdM tengan instalados programas antivirus y de protección del teclado antes de proceder a la instalación del sistema IdM. Conviene asegurarse de que el entorno de alojamiento no corra peligro de ataques de seguridad antes de instalar y utilizar el sistema IdM.

9.1.4 Almacenamiento seguro

Las bases de datos y los servidores de directorio contienen muchos datos importantes y delicados. Durante la configuración, el servidor de almacenamiento debe instalarse en un computador seguro y debe crearse una cuenta de administrador de conformidad con la guía de instalación adecuada, para impedir que pueda abrirse una cuenta maligna que luego ponga en peligro el sistema.

9.2 Directrices de seguridad para la utilización de los sistemas IdM

En la presente cláusula figuran directrices de seguridad para la utilización del sistema IdM. Uno de los principales problemas que hay que resolver es la autentificación y el control de acceso.

9.2.1 Firma digital

La firma digital es el mecanismo de seguridad que garantiza la autenticidad y la integridad de un mensaje firmado. En el sistema IdM existen muchas situaciones en las que el usuario tiene que demostrar su voluntad o consentimiento para que se efectúen las transacciones digitales. En tal caso, la firma digital se utiliza como prueba para verificar su integridad.

9.2.2 Encriptación

Los sistemas IdM requieren la utilización de encriptación a diversos niveles de funcionamiento. En primer lugar, los mensajes confidenciales que intercambian las entidades tienen que estar encriptados, pues se requiere confidencialidad. Dependiendo de la política de funcionamiento del IdM, algunos datos almacenados en las bases de datos también tienen que estar encriptados para garantizar la confidencialidad e impedir el acceso no autorizado. La encriptación proporciona el nivel máximo de confidencialidad del sistema IdM y, en última instancia, garantiza la privacidad de la información del usuario y de su identidad.

9.2.3 Autentificación

La autentificación es una función de control para impedir el acceso no autorizado al sistema por parte de usuarios ilegítimos. Con Internet, se recurre corrientemente a una autentificación sencilla que consiste en un identificador y una contraseña, pero tiene muchos puntos débiles en cuanto a la seguridad. Por consiguiente, se recomienda una autentificación rigurosa siempre que sea necesario garantizar un nivel alto de confianza de los usuarios que acceden al sistema. La autentificación mutua permite contrarrestar los ataques de peska (*phising*) y kosecha (*pharming*).

9.2.4 Comunicación segura

Mucha de la información que se intercambian entre el usuario y el sistema IdM es de carácter privado y confidencial. Además, los mensajes de protocolo entre las entidades pueden transportar información sensible y confidencial que es preciso encriptar para transmitirla por líneas de comunicación. La comunicación segura puede lograrse mediante tecnologías existentes tales como SSL y VPN.

9.2.5 Control de acceso

Diversas entidades, tales como administradores y usuarios, pueden acceder a un sistema IdM para utilizar servicios concretos y efectuar el mantenimiento cotidiano. Para impedir la penetración en el sistema por parte de terceros malignos se requiere algún mecanismo de control de acceso adecuado.

En muchos casos basta con recurrir al control de acceso discrecional (es decir, listas de control de accesos). Ahora bien, el modelo de control de acceso basado en la función puede proporcionar un control más completo y preciso, por lo que puede recurrirse a éste cuando se requiera un modelo de control de acceso más seguro y flexible.

9.3 Directrices de seguridad para servidores IdM

En esta cláusula se proporcionan directrices de seguridad que son específicas de los servidores IdM instalados y utilizados en estaciones de trabajo o servidores grandes.

9.3.1 Protección del sistema operativo

La mayoría de los servidores IdM disponibles suelen funcionar en un sistema operativo (OS) de propósito general. Muchos problemas de seguridad pueden evitarse con una correcta configuración del sistema operativo empleado por el servidor IdM. Dado que el servidor IdM corre sobre un sistema operativo existente, su seguridad depende principalmente de dicho sistema operativo. Las técnicas para proteger los diversos sistemas operativo son muy variadas, por lo que en esta cláusula se indican procedimientos genéricos que suelen utilizarse para proteger la mayoría de los sistemas operativos. Los fundamentos básicos de la gestión de seguridad del sistema operativo figuran en [UIT-T X.1205] y [b-NIST SP 800-123].

Para proteger los servidores IdM, es preciso proteger el sistema operativo siguiendo las siguientes etapas:

– aplicar los parches y las actualizaciones del sistema operativo;
– fortalecer y configurar el sistema operativo para tener en cuenta adecuadamente la seguridad;
– instalar y configurar controles de seguridad adicionales, en caso necesario;
– efectuar pruebas de la seguridad del sistema operativo para garantizar que los pasos anteriores ofrezcan una protección adecuada contra todos los problemas de seguridad.

9.3.2 Autentificación de usuarios con derechos para modificar la configuración

En los servidores IdM, los usuarios autorizados a configurar el servidor debe limitarse a unos cuantos administradores del servidor designados. Para aplicar las restricciones de política que se estimen necesarias, el administrador del servidor debe configurarlo para que exija la autentificación de usuarios, que habrán de demostrar que están autorizados para tal acceso. En el caso de que los servidores IdM tengan que proporcionar niveles de confianza y garantía elevados, las organizaciones también pueden recurrir a dispositivos de autentificación resistentes, tales como testigos o dispositivos de contraseña volátil. En este caso, se desalienta la utilización de mecanismos de autentificación en los que la información de autentificación se vuelve a utilizar (por ejemplo, contraseñas) y se transmite en formato de texto sin protección por una red no fiable, dado que la información puede interceptarse y ser utilizada por un agresor para hacerse pasar por un usuario autorizado.

La configuración por omisión del sistema operativo suele incluir cuentas de invitados con o sin contraseña. El administrador debe suprimir o desactivar las cuentas de invitados que no se utilicen para impedir que las empleen los agresores.

9.3.3 Control de acceso en modo configuración

Muchos de los servidores IdM ofrecen la capacidad de especificar privilegios de acceso individuales para credenciales e información sobre identidad. Todo usuario que tenga acceso al servidor IdM no debe estar autorizado a acceder a otra información sobre la identidad de los usuarios. La configuración adecuada de los controles de acceso puede ayudar a impedir la divulgación de información sensible o restringida sobre la identidad que no debe divulgarse.

También pueden utilizarse los controles de acceso para limitar la utilización de recursos en caso de ataque de DoS (denegación del servicio – *denial of service*) contra el servidor.

9.3.4 Registro

El registro es una de las medidas de seguridad más importantes. Es fundamental registrar los datos correctos y luego supervisar meticulosamente dichos registros. En caso de comunicaciones encriptadas son importantes los registros de red y de sistema, especialmente estos últimos, ya que la supervisión de la red resulta menos eficaz.

El análisis de los registros es obligatorio y una manera efectiva de detectar actividades sospechosas. En muchos casos, los ficheros registro son la única prueba de un comportamiento sospechoso. Al activar los mecanismos para registrar información se consigue utilizar los registros para detectar intentos de intrusión fallidos y exitosos e iniciar mecanismos alerta cuando se necesita efectuar una investigación más profunda. Se debe disponer de procedimientos y herramientas para procesar y analizar los ficheros registro y para examinar las notificaciones de alerta.

Se ha de velar por que los controles de acceso apliquen la separación de tareas de modo que los registros del servidor no puedan ser modificados por los administradores del mismo y asegurarse de que sólo los procesos del servidor puedan añadir información a dichos ficheros registro.

9.4 Directrices de seguridad para clientes IdM

En esta cláusula figuran directrices de seguridad para los programas cliente IdM. En el caso de que como cliente IdM se utilice un navegador web, la vulnerabilidad depende del navegador propiamente dicho. Sin embargo, sigue siendo posible aplicar algunas de las directrices para garantizar la seguridad de su entorno cliente.

9.4.1 Distribución segura de un programa cliente

Hoy en día muchos de los aplicativos que dependen del navegador se descargan por la web. Si un usuario descarga por error un programa cliente IdM equivocado que puede dañar el sistema del usuario, ningún mecanismo de seguridad robusto será capaz de proteger al usuario contra la actividad maliciosa. Por consiguiente, el proveedor de un programa cliente IdM debe garantizar la protección de la integridad del programa cliente que distribuye y ofrecer una forma segura de validar su integridad.

9.4.2 Integridad de un programa cliente

Para garantizar la integridad de un programa cliente, la mejor solución es una firma digital. Si el programa cliente está firmado por un proveedor y se proporciona un certificado de firma para su validación, el usuario podrá descargarlo y verificar la integridad del código del programa. Existe un método alternativo que consiste en utilizar un algoritmo de generación numérica (*hash*) para garantizar la integridad del código. El código del cliente se emplea como parámetro de entrada de dicho algoritmo y se obtiene un valor, que constituye el compendio del código del cliente. Si el valor generado se publica en la web de manera segura, el usuario puede validar su programa cliente calculando el valor generado por el programa cliente descargado. Ahora bien, el primer método es más seguro que este último.

9.4.3 Fichero de base de datos cliente

Los ficheros de base de datos cliente deben almacenarse en un lugar seguro. El acceso a la base de datos debe limitarse exclusivamente a los usuarios autentificados. En muchos casos, los clientes IdM gestionan la información de credenciales usuario, en particular las contraseñas y los testigos de seguridad que deben mantenerse encriptados para garantizar su confidencialidad. Asimismo, el propio fichero de base de datos debe protegerse contra la alteración ilícita y la modificación en aras de su integridad. Cuando el fichero de base de datos se borra del sistema, no debe quedar ningún rastro en el disco duro que permita su recuperación ulterior.

9.4.4 Contraseñas seguras

Buena parte del mecanismo de seguridad depende en última instancia de una contraseña de autentificación para acceder al sistema. Si el usuario utiliza una contraseña débil que puede piratearse mediante un ataque exhaustivo, no existe ningún otro mecanismo de seguridad que pueda proteger el sistema contra los usuarios malignos. Así pues, la tarea más importante del proveedor de servicios IdM es velar por que los usuarios utilicen contraseñas fuertes para el inicio de sesión.

9.4.5 Desinstalación de un programa cliente

Al desinstalar un programa cliente en un sistema de usuario, deberán suprimirse de manera permanente todas las contraseñas, credenciales e información sobre la identidad, así como la configuración personal del programa cliente.

9.5 Directrices de seguridad para los clientes IdM móviles

En esta cláusula figuran las directrices de seguridad para los clientes IdM móviles que se instalan y utilizan en un dispositivo móvil. El dispositivo móvil tiene características particulares tales como la portabilidad y la movilidad. Ahora bien, estas características constituyen puntos débiles por lo que a la seguridad se refiere, que puede explotar el agresor.

9.5.1 Pérdida o robo del dispositivo

Como el dispositivo móvil es portátil, es muy probable extraviarlo o que lo roben. Existen muchas formas de manipular el dispositivo móvil con objeto de obtener información personal para robar la identidad. Por consiguiente, el cliente móvil en el dispositivo debe estar preparado contra cualquier tipo de ataque que pueda causar la utilización no autorizada o el robo de identidad. En caso de extravío o robo del dispositivo, se informará de ello al proveedor de comunicaciones móviles, y habida cuenta de la situación, el operador puede bloquear el dispositivo a distancia para impedir cualquier acceso al mismo. Esta medida resulta adecuada cuando el dispositivo se pierde en el entorno próximo, como en casa o en el lugar de trabajo. En cualquier otro caso, si el propietario estima que el dispositivo ha sido perdido o robado de manera permanente y que no existe forma alguna de recuperarlo, el operador debe ser capaz de borrar toda la información personal y el registro de identidad almacenado en el dispositivo.

9.5.2 Autentificación de dispositivos

Si el dispositivo móvil tiene una pantalla de tamaño muy pequeña para la introducción de texto, resulta muy difícil para el usuario iniciar la sesión utilizando una contraseña alfanumérica cada vez que lo vaya a utilizar. En este caso, se utiliza como contraseña el número de identificación personal (PIN, *personal identification number*), aunque en muchas ocasiones no se utilice por razones de costo o de conveniencia. Para superar esta situación, el cliente móvil IdM debe proporcionar mecanismos de autentificación fácil de utilizar y a la vez lo suficientemente seguro para el dispositivo móvil. El cliente móvil debe exigir la autentificación mediante contraseña en caso de que el dispositivo no utilice ningún mecanismo de autentificación para el inicio de sesión del usuario.

9.5.3 Copia de seguridad de la base de datos

La mayoría de la información sobre la identidad para diversos servicios se recopila y procesa mediante un dispositivo móvil. Ahora bien, muchas de estas identidades contienen información personal privada y sensible, por lo que resulta imprescindible proteger su integridad y confidencialidad. Como se indicó anteriormente, es muy fácil extraviar o robar el dispositivo. Por consiguiente, el cliente móvil de Gilbert debe disponer de un mecanismo para poder hacer copias de seguridad de la base de datos que contiene la información de identidad. Esto puede realizarse de dos maneras. La primera consiste en guardar la copia de seguridad de la base de datos en un medio de almacenamiento secundario, por ejemplo una tarjeta de memoria SD (*secure digital*), si se dispone de ella. La segunda forma consiste en utilizar un servidor externo que suministra el servicio de

copia de seguridad de la base de datos para el cliente. En este caso siempre es posible restablecer la base de datos del usuario, aun cuando el dispositivo haya sido extraviado o robado.

9.5.4 Seguridad de las comunicaciones móviles

Los dispositivos móviles utilizan la mayor parte del tiempo comunicaciones móviles para comunicarse con otros dispositivos. Ahora bien, se reconoce que las comunicaciones móviles son muy vulnerables a los ataques activos y pasivos. El cliente móvil IdM suele transmitir información personal sensible por la red móvil. Por consiguiente, toda comunicación con el cliente móvil utilizando el enlace móvil debe protegerse mediante mecanismos de seguridad en la capa de transporte a fin de garantizar su integridad y confidencialidad.

9.6 Consideraciones relativas a la privacidad en los sistemas IdM

La privacidad es una cuestión muy importante en el contexto de la seguridad IdM. Ahora bien, cada país dispone de sus propias normativas y reglamentos relativos a la aplicación en la práctica de las directrices sobre privacidad. Por consiguiente, en esta cláusula se analizan y exponen a título informativo algunas de las cuestiones de privacidad para los sistemas IdM.

9.6.1 Consentimiento del usuario

Cuando se recaba la identidad de un usuario y es utilizada por un IDP o SP, debe obtenerse explícitamente su consentimiento. Lo ideal sería obtener el consentimiento del usuario mediante algún tipo de firma digital, que pueda verificarse posteriormente en caso necesario.

9.6.2 Selección de la identidad

Los sistemas IdM ofrecen explícitamente un mecanismo para que cada persona pueda autorizar o no la recopilación, utilización, transferencia, almacenamiento, archivado o eliminación de la identidad. De este modo se aumenta su privacidad, por cuanto es el propio usuario quien controla la gestión de la política de privacidad e identidad. Este método centrado en el usuario debe tenerse en cuenta durante la fase de diseño del sistema IdM.

9.6.3 Objeto de la identidad

Antes de recabar su identidad, el sistema IdM debe notificar al usuario la finalidad para la cual se recaba y utiliza la información personal, de manera fácilmente comprensible. Asimismo, el sistema debe tratar de utilizar la identidad para los fines notificados.

9.6.4 Limitación y minimización de la identidad

Los sistemas IdM que recaban identidades deben obtener únicamente las necesarias para llevar a cabo las tareas previstas, a menos que dispongan del consentimiento del individuo o lo permita o exija la ley.

El sistema IdM que recaba identidades debe examinar y documentar en detalle los procedimientos que estipulen claramente qué información de identidad se necesita y para qué fines, además de cómo se garantiza que el procesamiento de la identidad recaba solamente las mínimas identidades necesarias.

9.6.5 Eliminación de la identidad

Los sistemas IdM deben eliminar la identidad una vez hayan terminado de utilizarla para los fines previstos y no existan otras prescripciones reglamentarias o jurídicas que exijan conservarlas durante un periodo de tiempo mayor. Al eliminar la identidad debe garantizarse que también se suprime toda la información de identidad almacenada en los sistemas conexos, tales como los sistemas de copia de seguridad y archivo.

9.6.6 Configuración de la política de privacidad

Antes de que el sistema IdM se ponga en funcionamiento, es necesario establecer políticas de privacidad como las relativas a las preferencias de privacidad y la autorización de privacidad. Estas políticas rigen la utilización de la identidad que el usuario envía al sistema.

9.6.7 Anonimato

El anonimato podría ser el objetivo último de todo sistema IdM de privacidad mejorada. Ahora bien, resulta muy difícil y complejo proporcionar esta función a un costo razonable. Por consiguiente, en la mayoría de los casos puede recurrirse a un seudónimo para satisfacer los requisitos de privacidad de un sistema IdM.

Bibliografía

[b-NIST SP 800-123] Scarfone, K.A., Jansen, W., and Miles, T. (2008), "*Guide to General Server Security*", NIST Special Publication SP-800-123.

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, 2012