Seguridad en Internet: un estado del arte

Ruben A. González García [*]
Selene Chaires Enríquez [**]
Universidad "Juárez" Autónoma de Tabasco, DACB
Carr. Cunduacán-Jalpa Km 1, Cunduacán Tabasco, México
A.P. 24 C.P. 86690. Tel.(+52)914 336-0928

Los servicios ofrecidos a través de Internet son de distinta naturaleza y cada uno de ellos tiene sus propios requerimientos de seguridad. Por ejemplo, la seguridad requerida por un sistema de control escolar en línea es diferente a la seguridad requerida por una aplicación de videoconferencia. Existe una gran variedad de mecanismos de seguridad disponibles para ser usados en Internet. En el presente documento se hace un estudio exploratorio de los mecanismos que, debido a sus características o a su popularidad, son los más importantes para garantizar algún nivel de seguridad en Internet.

The services offered through Internet are of different natures and each one of them has its own requirements for security. For example, the security required by an in-line scholastic control system is different from the security required by a videoconference. A great variety of security mechanisms exists for the Internet. In this paper, an exploratory study of the more important mechanisms to guarantee some level of security on the Internet is made.

Palabras clave: Seguridad, Internet
Keywords: Security, Internet

1. Introducción

El uso creciente de Internet para actividades que van más allá de la comunicación personal y el entretenimiento ha generado una creciente demanda de seguridad en la red. El comercio electrónico en sus diferentes modalidades, las transacciones bancarias, la certificación de componentes descargables de la red[1], los servicios de extranet, las redes privadas virtuales y los portales Web en general, son algunas de las aplicaciones de Internet que requieren mayores niveles de seguridad para garantizar su correcto funcionamiento.

La seguridad en redes involucra diferentes aspectos tales como:

- **Privacidad:** protección de la información contra accesos no autorizados.
- **Integridad:** prevención de la información en contra de modificaciones no autorizadas.
- **No rechazo de servicio:** evitar que a un usuario legítimo le sea denegado el acceso a un servicio disponible.
- **No repudio de autoridad:** evitar que un usuario niegue ser el autor de la información él mismo generó.

[*] ruben.gonzalez@basicas.ujat.mx
[**] sele_chaires@hotmail.com
[1] Por ejemplo, los controles ActiveX

- **Disponibilidad de los servicios:** evitar que un servicio sea inhabilitado ilegalmente.

La naturaleza de cada servicio determina las características de la seguridad requerida. Por ejemplo, un servicio de correo electrónico no requiere las mismas condiciones de seguridad que un servicio de banca en línea.

A través de los años, la comunidad Internet ha desarrollado diversos mecanismos de seguridad para aplicaciones específicas incluyendo correo electrónico, aplicaciones cliente servidor y acceso Web [1], basados en tres elementos fundamentales: encriptación, autenticación e integridad [4].

A continuación se presenta una breve descripción de estos mecanismos.

2. IPsec

IPsec (*Internet Protocol Security*) es un protocolo diseñado para proveer servicios de seguridad en la capa de red. IPsec se encuentra ubicado directamente encima del protocolo IP, por debajo de los protocolos TCP y UDP. Los servicios que proporciona son:

1. Control de acceso
2. Integridad
3. Autenticación de origen de datos
4. Rechazo de paquetes repetidos
5. Confidencialidad (encriptación)
6. Confidencialidad de un flujo limitado de tráfico

Los componentes básicos de IPsec están basados en los siguientes protocolos:

AH (*Authentication Header*) es un protocolo que porporciona los servicios de autenticación de datagramas IP. El encabezado IP se encapsula con los datos, dentro de la trama IP. AH proporciona soporte para la integridad y autenticación de datos mediante funciones resumen (*Hash*) y protocolos de autenticación simple.

ESP (*Encapsulating Security Payload*) es un protocolo que proporciona el servicio de confiabilidad de los datagramas mediante el cifrado de los datos usando criptografía asimétrica[2]. Al igual que con AH, el encabezado ESP se coloca dentro del datagrama IP junto con los datos.

ISAKMP/Oakley (*Internet Security Association and Key Management Protocol/Oalkey*) es el protocolo por omisión para la administración de las claves públicas utilizadas por AH y ESP. ISAKMP/Oakley está formado precisamente por los protocolos Oakley e ISAKMP. Oakley es un protocolo de intercambio de llaves basado en una versión mejorada del algoritmo de Diffie-Hellman. ISAKMP es un

[2]También conocido como criptografía de clave pública

marco de trabajo para la administración de claves en Internet, definiendo formatos para negociación y atributos de seguridad [1].

IKE (*Internet Key Exchange*) es otro protocolo para administración de claves tanto para AH como para ESP [5].

Los protocolos AH y ESP pueden realizar transferencias tanto en modo **transporte** como en modo **túnel**. En el primer caso, la encriptación se realiza en la capa de transporte (TCP o UDP, solo se encriptan los datos), mientras que en el segundo caso la encriptación se lleva a cabo en la capa de red (IP, se encriptan los datos y encabezados).

El protocolo IPsec forma parte del estándar IP v6, sin embargo fue diseñado para funcionar también con la versión 4 del protocolo IP.

3. Administración de claves

Además de ISAKMP/Oakely e IKE los cuales están diseñados para operar con el protocolo IPsec (capa de Red), existen otros servicios de administración de claves públicas diseñados para operar con las aplicaciones. La idea generalizada subyacente en todos estos protocolos es la existencia de una autoridad confiable que garantiza (certifica) la identidad de los participantes en una sesión de comunicación, mediante algún algoritmo de distribución de claves.

Los servicios que estos sistemas pueden ofrecer son:

- Autenticación (AU)
- Confidencialidad de datos (CD)
- Integridad de datos (ID)
- Control de acceso (CA)
- No rechazo de servicio (NR)

Los principales sistemas estándares de distribución de claves públicas son:

- **Kerberos**: disponible comercialmente y de forma gratuita. Ofrece los servicios AU, CD e ID
- **NetSP**: disponible comercialmente. Ofrece los servicios AU, CD e ID
- **SPX**: disponible de manera gratuita. Ofrece los servicios de AU, CD e ID
- **TESS**: disponible comercialmente ofrece los servicios de AU, CD, ID y NR
- **SESAME**: disponible de manera comercial y gratuita. Ofrece los servicios AU, CD, ID y CA
- **OSF DCE**: es un estándar comercial que ofrece los servicios de AU, CD, ID y CA [4]

La utilización de estos sistemas de seguridad no es transparente para los desarrolladores de aplicaciones, quienes deben incluir en sus programas el código cliente de estos servicios. Debido a esta situación y al hecho de que ninguno de los protocolos mencionados ha logrado posicionarse de manera dominante en el campo de la seguridad, el uso de estos sistemas en Internet es bastante esporádico.

4. Secure Socket Layer (SSL)

Uno de los servicios más utilizados en Internet es el World Wide Web (Web). El WWW a su vez sirve como plataforma para una gran diversidad de servicios, cada uno de los cuales tiene ciertos requerimientos específicos en cuanto a seguridad. Con la aparición del comercio electrónico y su rápido crecimiento, surgió la necesidad de crear mecanismos apropiados para garantizar que las transacciones comerciales entre los proveedores de servicios y sus clientes se lleve a cabo de manera confiable.

En respuesta a esta necesidad, Netscape diseñó SSL, un protocolo que trabaja sobre TCP en la capa de sesión. SSL está diseñado para proporcionar un servicio confiable de extremo a extremo. En realidad SSL incluye varios protocolos dedicados a diferentes funciones. El objetivo de SSL es establecer sesiones confiables entre clientes y servidores, usando conexiones TCP. Las principales funciones de SSL son:

- Establecimiento de conexión
- Cifrado de datos (confidencialidad)
- Integridad de los datos

SSL puede utilizar diferentes algoritmos para el cifrado de datos como IDEA, RSA, DES y Fortezza entre otros, así como los esquemas de codificación de flujo y de bloques.

Por otro lado, TLS (*Transport Layer Security*) es el nombre oficial que recibe SSL en los estándares de Internet.

En la actualidad SSL es uno de los protocolos de seguridad más utilizado en aplicaciones WWW, excepto en comercio electrónico.

5. Otros algorítmos criptográficos

Adicionalmente, existen otros algoritmos criptográficos orientados hacia aplicaciones específicas, entre los que destacan:

SET: (*Secure Electronic Transaction*) es un estándar abierto creado conjuntamente por VISA y Master Card. Se trata de un protocolo de seguridad orientado hacia los servicios de pagos electrónicos mediante el uso tarjetas de crédito bancarias. SET proporciona integridad de mensajes, autenticación de datos financieros y encriptación de información sensible [3].

PGP: (*Pretty Good Privacy*) Es un algoritmo de cifrado de clave pública orientado hacia aplicaciones de correo electrónico. PGP combina el algoritmo IDEA de clave privada con el RSA de clave pública y el MD5 para firmas digitales.

6. Firewalls

Un firewall (cortafuego) es un dispositivo de seguridad que controla el flujo de paquetes de datos entre dos redes. El objetivo principal de un firewall es proteger una red de otra. Para proteger la red de una empresa, típicamente se coloca un firewall entre la red interna de la empresa y el Internet [5].

Un firewall debe cumplir con las siguientes características generales:

- Todo el tráfico de adentro hacia fuera y viceversa, debe pasar a través del firewall.
- Solamente el tráfico autorizado, según la política de seguridad definida, podrá pasar a través del firewall.
- El firewall en sí mismo debe ser inmune a cualquier tipo de penetración [1].

Un firewall monitorea y filtra todo el tráfico que entra y sale de una red. Para ello se emplean tres diferentes tipos de filtrado o alguna combinación de ellos [5]:

1. **Filtrado de paquetes IP:** consiste en el análisis de la información contenida en las cabeceras de los datagramas IP y la eliminación o retransmisión de los mismos en base a la direcciones fuente y destino.
2. **Filtrado a nivel de aplicación (servidores Proxy):** este filtrado implica el bloqueo de la totalidad los datagramas IP transmitidos entre la red interna e Internet. En este caso, los clientes internos establecen conexión con el firewall y le hacen peticiones; este, actuando como intermediario, establece conexiones con los servidores externos y les envía peticiones. Las respuestas recibidas por el firewall son retransmitidas a los clientes. En este tipo de firewalls debe existir un proxy para cada protocolo de aplicación que desee accesar la red externa (http, telnet, ftp, smtp, etc.). La operación de los proxys es transparente para los servidores externos, pero no para las aplicaciones clientes que están dentro de la red protegida por el firewall, las cuales deben ser configuradas para ello.
3. **Filtrado de conexión (circuito):** este tipo de firewall controla la conexión entre un cliente y un servidor, y no el intercambio de paquetes entre ellos [5].

Los firewalls de filtrado de paquetes IP se utilizan a menudo como primer nivel de defensa contra una red no confiable. Si bien es cierto que el método de filtrado de paquetes proporciona una manera eficiente, transparente y general de controlar el tráfico en la red, también es cierto que este método no exige muchos requisitos de seguridad, debido a que cuenta con información incompleta para trabajar. Solamente la información de las capas de red y transporte del modelo OSI, como direcciones IP, números de puerto e indicadores TCP, está disponible para decisiones de filtrado. Debido a la falta de información de contexto, ciertos protocolos como UDP y RPC

son más difíciles de filtrar de manera efectiva. De ahí la importancia de complementar el filtrado de paquetes con el filtrado a nivel aplicación y a nivel conexión [6].

Existe un cuarto tipo de firewall conocido como bastión. Un host bastión es un sistema identificado por el administrador de la red como un punto crítico en la seguridad de la misma. Típicamente, el bastión sirve como una plataforma para un gateway a nivel de aplicación o a nivel de circuito. Las características más importantes de un bastión son:

- La plataforma hardware del host bastión ejecuta un sistema operativo seguro y confiable.
- Solamente se instalarán en el host bastión los servicios que el administrador de la red considere esenciales.
- Un bastión puede requerir autenticación adicional antes de que a un usuario se le autorice el acceso a los servicios proxy.
- Cada proxy es configurado para soportar solamente un subconjunto de la funcionalidad y de los comandos de la aplicación estándar.
- Además, cada proxy es configurado para proporcionar acceso únicamente a ciertos hosts específicos.
- Cada proxy en el bastión, lleva una bitácora detallada de su actividad [1].

La seguridad real que pueda brindar un firewall, depende no solamente de su configuración, sino también de las políticas de seguridad y de las prácticas de los usuarios. Entre las principales limitaciones de un firewall, se tiene que:

- Un firewall no puede proteger la red en contra del tráfico que entra directamente a esta por algún otro punto.
- Un firewall no puede proteger en contra de usuarios internos mal intencionados o peligrosos.
- Un firewall no puede proteger en contra de la transferencia de virus.

7. Otros mecanismos de seguridad

Otros mecanismos de seguridad que estan siendo ampliamente utilizados son:

RADIUS: (Remote Authentication Dial-In User Service) es una norma orientada hacia el control de accesos remotos a Internet a través de líneas telefónicas conmutadas y redes inalámbricas. Los servicios que ofrece son autenticación, autorización y contabilidad del servicio.

VPNs: (*Virtual Private Networks*) son redes que ofrecen las características de seguridad de una red privada a pesar de operar sobre redes públicas como Internet. Las VPNs se basan en el uso de túneles, cifrado de datos, mecanismos de autenticación, distribución de claves públicas e incluso de firewalls para ofrecer una canal de conumicación seguro entre sus usuarios. Uno de los protocolos más usados para crear VPNs es IPsec.

Existen otras herramientas administrativas como las bitácoras y la auditoría que ayudan a detectar violaciones a la seguridad y condiciones de riesgo, con la finalidad de prevenir futuros incidentes.

8. Conclusión

Garantizar la seguridad de la información y de los servicios disponibles a través de Internet es una tarea sumamente complicada pero necesaria para soportar la evolución de los servicios existentes y la aparición de nuevos servicios.

Internet es un sistema sumamente complejo debido la gran cantidad de conceptos y tecnologías involucradas, y a la presencia de los imponderables errores humanos que suelen existir en el hardware y sobre todo en el software de las computadoras [8].

Los diversos mecanismos de seguridad presentados en este documento satisfacen en gran medida las necesidades de seguridad de los servicios actuales pero no de sus usuarios quienes, debido a cuestiones culturales, aun desconfian de los servicios financieros en línea y del comercio electrónico.

En un mundo cambiante, donde la tecnología evoluciona diariamente, la seguridad no es algo que pueda alcanzarse de manera absoluta, sino un proceso continuo; es algo que debe evolucionar constantemente, no solo para subsanar las deficiencias de los sistemas existentes, sino para tratar de anticipar las necesidades futuras. Probablemente hoy en día ninguna persona se atrevería a confiar la vida de un familiar enfermo de deficiencia renal crónica a un equipo de diálisis peritoneal controlado desde un hospital remoto a través de Internet, pero en el futuro... tal vez si.

Referencias

[1] Stallings, W., *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2^{nd} edition, 1999

[2] IEC, *Internet Security*

[3] IEC, *Electronic Commerce*

[4] Oppliger, R., *Sistemas de Autentificación para Seguridad en Redes*. Alfaomega 1998

[5] Mariño, P., *Las comunicaciones en la empresa. Normas, redes y servicios*. (Ra-Ma) 2^a edición (408-409)

[6] Siyan, K.; Hare, C.*Firewalls y la seguridad en Internet*. (Prentice-Hall) 2^a edición. (325-354)

[7] Understandig Vitual Private Networking
http://www.adtran.com/all/Doc/0/EU0GPR0PEFB139RF038BE81ID8/EN286.pdf

[8] The Twenty Most Critical Internet Security Vulnerabilities (Updated) http://www.sans.org/top20/