

Seguridad en Internet

**Integrantes:** Yanko Arévalo – 2821044-2

Marco Encina – 2821066-3

Evandry Ramos – 2821002-7

**Fecha:** 30 de julio de 2012

**Nombre profesor:** Agustín González

**Ayudantes:** Constanza Valdés

Adán Morales

**Resumen**

En el trabajo realizado se tratarán temas relevantes a la seguridad en Internet, con fines de compartir información confidencial entre los host terminales o routers de forma segura, evitando ataques o intercepción de mensajes por parte de terceros. Se tratarán temas referidos a la encriptación de paquetes y a la autenticación de un equipo o persona antes de comenzar la transferencia de información, así como también se dará un visión general sobre los aspectos que se deben considerar en cuanto a los protocolos de seguridad existentes actualmente en Internet.

**Introducción**

El uso actual de Internet no cubre sólo el intercambio de información pública para todos los usuarios, sino que también es utilizado para mensajería electrónica, transacciones bancarias, información de gobierno, etc. Por esta razón, se busca que la comunicación de datos privados entre usuarios o entre un usuario y un servidor sea vista o interpretada sólo por ambos.

La seguridad en Internet, es entonces, un tema de constante preocupación para mantener la transmisión de datos privados. En el transcurso del tiempo se observa que las técnicas de seguridad en Internet deben ser mejoradas, debido a que los hackers poseen conocimiento cada vez más sofisticado sobre los protocolos que rigen la seguridad, y van mejorando las técnicas para captar mensajes privados.

**Seguridad en Internet**

Supóngase que el equipo A y el equipo B desean comunicarse entre sí y desean hacerlo de forma segura. Puede tratarse de dos routers que intentan traspasarse sus tablas de ruteo de forma segura, un cliente y un servidor que quieren establecer una conexión de transporte segura, o dos aplicaciones de correo electrónico que desean intercambiar correos, de manera segura.

Los asuntos de amores ilícitos, las comunicaciones en tiempos de guerra y las transacciones de negocios son necesidades humanas de comunicaciones seguras comúnmente buscadas.

Algo que se ha repetido en los párrafos anteriores, es el concepto de comunicación de forma “segura”, que es una característica de una comunicación que posee muchas caras.

De hecho, unos equipos A y B desearán que el contenido de su comunicación permanezca en secreto para un equipo tercero escondido. Además, probablemente, querrán estar seguros de que cuando estén comunicándose, lo estén haciendo en efecto con el otro, y si su comunicación es alterada por un tercero, puedan darse cuenta de tal manipulación.

Dadas estas premisas, es posible identificar las propiedades deseables de una “comunicación segura”

* **Confidencialidad:** Únicamente el emisor y el receptor deseado deberán ser capaces de entender el contenido del mensaje transmitido. Como los oyentes ocultos pueden interceptar el mensaje, se requiere necesariamente que este sea encriptado (disfrazado) para que el mensaje no pueda ser desencriptado (entendido) por algún ente externo.
* **Autenticación:** Un equipo, como emisor y receptor, debería ser capaz de confirmar la identidad de la otra parte involucrada en la comunicación para asegurarse de que la otra parte es en efecto quién o lo que parece. La comunicación cara a cara resuelve esto, mediante reconocimiento visual, sin embargo cuando los entes no se ven directamente la autenticación no es tan simple.
* **Integridad del Mensaje:** Incluso si el emisor y el receptor no son capaces de autenticarse entre ellos, también querrán estar seguros de que el contenido de sus comunicaciones no es alterado durante la transmisión, ya sea maliciosamente o por accidente. Además, un receptor querrá comprobar que un mensaje ha llegado desde un supuesto emisor.
* **Disponibilidad y Control de Acceso:** La necesidad de seguridad en la redes se ha hecho muy patente en los últimos años debido a los DoS (Denial of Service), que han conseguido que una red, un host u otra pieza de la infraestructura de la red dejaran de ser utilizables por sus legítimos usuarios.

La confidencialidad, autenticación e integridad del mensaje han sido considerados componentes clave de la comunicación segura por bastante tiempo. La disponibilidad y el control de acceso son extensiones más recientes de la noción de comunicación segura, motivadas por los aspectos de la realidad que obligan a la seguridad de la infraestructura de la red contra un potencial ataque de hackers con malas intenciones.

**Encriptación**

Como se dijo anteriormente, la criptografía es el medio por el cual la información se hace ininteligible a intrusos, esto para preservar tanto la confidencialidad de la comunicación, como la autenticación, es decir, los interlocutores quieren garantías de que la comunicación con la persona ó máquina al otro lado de la red sea privada, y que tampoco pueda ser manipulada por un tercero.  
Antes de hablar de los distintos algoritmos de encriptación, es necesario hablar del concepto de clave simétrica. Si se tiene un mensaje m y Alicia lo encripta por medio de una clave K1 (es decir K1(m)), luego lo envía a Roberto y él lo traduce con una clave K2, tal que K2(K1(m))=m, se tendrá un sistema de clave simétrica en el cual las claves K1 y K2 son idénticas y secretas.

Para lograr esto existen diversos algoritmos de clave simétrica, mediante los cuales un mensaje es cifrado para tener una transmisión segura. Los primeros algoritmos de encriptación datan de la antigua Roma, este primer algoritmo es conocido como *cifrado Cesar.*  
El *cifrado Cesar* consiste en tomar cada letra del abecedario e intercambiarla por la k-ésima letra siguiente, es decir, k es la llave del algoritmo. Por ejemplo, si se usa k=2, el texto “*Hola mundo”*  quedaría “*Mtpf qzrit”.* La robustez de este algoritmo es muy baja, ya que solo existen 27 posibles llaves, por lo que este algoritmo solo sirve para ilustrar lo que es la encriptación.  
Otra posibilidad es el *cifrado*  *monoalfabético,* el cual es bastante parecido al cifrado Cesar, pero este algoritmo asigna una llave distinta a cada letra, lo que resulta en 27! (aproximadamente 1027) posibles llaves, en este caso “*Hola mundo”* quedaría “*Akgm hyjvk”,* aunque este algoritmo tiene una mayor dificultad para ser roto, con los medios modernos este algoritmo es relativamente fácil descifrar.

Una revisión más robusta de estos algoritmos es el *cifrado polialfabetico,* en este caso se emplean distintas cifras monoalfabeticas siguiendo un patron, codificando cada letra en una posición determinada dentro del mensaje. De esta manera, la misma letra sera codificada en forma distinta dependiendo la poscición. En este caso, usando k1=5, k2=19 y con un patrón k1, k2, k2, k1, k2; *“Hola mundo”* quedaría “*Mtqf rzsih”.*

**- Estándares de encriptación.**

El primer estándar de encriptación usado ampliamente y creado en 1977 es el *Data Encryption Standart* (DES), un estándar de clave simétrica que toma el texto sin codificar en bloques de 64 bits, 8 bits de paridad (1 bit por cada byte de datos) y 56 bits de clave. Básicamente, el objetivo de este algoritmo es revolver el texto sin cifrar y la clave para que cada bit del texto cifrado dependa de cada bit de datos y de cada bit de clave, para la implementación se realiza una permutación entre los bits de datos, y un se cifra solo una cierta parte con solo 48 de los 56 bits de clave, luego se repiten los pasos anteriores 16 veces para formar la salida cifrada de 64 bits. En los casos en que se necesita una seguridad de mayor orden el algoritmo en si puede ser iterado para aumentar su seguridad, es así como existe también el estándar 3DES, el cual es un estándar de alta seguridad consistente en iterar 3 veces el algoritmo DES.

En 2001, se creo el estándar de encriptación avanzada (AES en inglés), este estándar de clave simétrica permite la encriptación en bloques de 128 bits de datos con claves de hasta 256 bits, se dice que una máquina capaz de romper DES de 56 bits en un segundo tardaría 149 billones de años en romper AES de 128 bits.

**- Clave pública o asimétrica**

El principal problema de los algoritmos de clave simétrica es que ambas partes deben ponerse de acuerdo sobre cual será la clave para realizar una conversación segura, la solución más elegante a este problema fue descrita en vez primera por Diffie y Hellman. En su algoritmo, la encriptación y desencriptación son realizadas por claves distintas y sólo la clave para encriptar la información es compartida con cualquier persona, así quien desee comunicarse con Roberto le solicitará su clave pública para enviarle mensajes encriptados con esta clave, y solo Roberto podrá ver su contenido desencriptándolos. Existen diversos algoritmos de clave pública ([Diffie-Hellman](http://es.wikipedia.org/wiki/Diffie-Hellman), [DSA,](http://es.wikipedia.org/wiki/DSA) [ElGamal,](http://es.wikipedia.org/wiki/ElGamal) [elíptica,](http://es.wikipedia.org/wiki/Criptograf%C3%ADa_de_curva_el%C3%ADptica)[Merkle-Hellman,](http://es.wikipedia.org/wiki/Merkle-Hellman) [Goldwasser-Micali,](http://es.wikipedia.org/w/index.php?title=Goldwasser-Micali&action=edit&redlink=1)[Goldwasser-Micali-Rivest, etc](http://es.wikipedia.org/w/index.php?title=Goldwasser-Micali-Rivest&action=edit&redlink=1)), sin embargo el algoritmo de uso común para esto es el algoritmo RSA, el cual se procede a explicar a continuación  
1- Escoja 2 números p y q tan grandes como sea posible, es decir, que el producto pq sea de aproximadamente 1024 bit, sin embargo mientras más grandes sean, tardará el algoritmo en cifrar y descifrar.

2- Calcule n=pq y z=(p-1)(q-1).

3- Escoja e<n tal que los factores de e sean distintos a los factores de z.

4- Busque d tal que (ed mod z) = 1.

5- La clave publica a compartir consiste en el par (n,e) y la clave privada es el par (n,d).

**Autenticación**

La autenticación se refiere al proceso de identificar la identidad de alguien, que puede ser un router, un equipo terminal o una persona que desea comunicarse con un servidor en una red en el instante de tiempo en el que se produce la comunicación.

Este proceso se lleva a cabo mediante distintos protocolos, los cuales dependen del requerimiento del cliente que implementa seguridad en su red para compartir archivos en Internet.

Los protocolos de autenticación son:

* **Protocolo de autenticación pa 1.0:**

Corresponde al protocolo más simple de autenticación. La persona que desde autenticarse envía un mensaje indicando su identidad a la persona o servidor con la cual desea establecer una comunicación, el cual capta el mensaje y autentifica al usuario.

* **Protocolo de autenticación pa 2.0:**

Corresponde a la autenticación mediante la dirección IP del usuario. El servidor, o persona que se comunica con un cliente, envía información o datos si la dirección IP que contiene el datagrama coincide con la dirección IP del usuario, la cual es conocida de antemano. Este protocolo resulta inseguro, puesto que es posible conocer la dirección IP de un equipo, así como también asignarla a algún equipo en específico, de forma que se puede captar un mensaje.

* **Protocolo de autenticación pa 3.0:**

Corresponde a la autenticación mediante la utilización de una contraseña conocida por el usuario y el servidor. Esta contraseña es enviada por el usuario al servidor y reconocida por este, antes de comenzar el intercambio de datos. La contraseña es enviada sin encriptar de un extremo a otro del enlace.

* **Protocolo de autenticación pa 3.1:**

Este protocolo es similar al protocolo pa 3.0, difiere únicamente en que la contraseña secreta es enviada encriptada al servidor y es desencriptada por este antes de comenzar la comunicación o intercambio de datos. Resulta, por ende, más seguro que el protocolo anterior, pues es seguro frente a interceptos de contraseña por parte de un intruso. La clave que se utiliza para encriptar la contraseña también es privada, es decir, sólo es conocida por el usuario y el servidor. Este protocolo puede sufrir un ataque de reproducción, es decir, un intruso capta la contraseña encriptada y la envía al servidor para recibir los datos enviados por éste al usuario.

* **Protocolo de autenticación pa 4.0:**

Corresponde a un protocolo de autenticación que utiliza contraseñas distintas en cada comunicación con el servidor. Estas pueden pertenecer a una secuencia de contraseñas o ser generadas por algún algoritmo. Este protocolo es utilizado principalmente para cerciorarse de que la comunicación con el usuario está ocurriendo en directo, es decir, la persona que se intenta autenticar corresponde realmente al usuario y no corresponde a una retransmisión de alguna autenticación pasada.

Se utiliza para esto un núnico, que consiste en un número que será utilizada sólo en una ocasión. El servidor envía un núnico al usuario, el cual lo recibe, encripta y envía de vuelta; el servidor desencripta el mensaje y comprueba que corresponda al núnico original. Luego, el núnico no se vuelve a utilizar, luego de finalizado su período de vida.

* **Protocolo de autenticación pa 5.0:**

Este protocolo utiliza la encriptación de contraseñas generadas en el instante de la comunicación, pero utilizando claves de encriptación públicas, para que no sea necesario acordar un clave secreta de encriptación entre el usuario y el servidor antes de comunicarse entre sí, que resulta en ocasiones, difícil. El proceso de autenticación es similar al señalado en el pa 4.0: El servidor envía un núnico generado al usuario, éste lo encripta con su clave privada y luego el servidor lo desencripta con la clave pública del usuario. Este protocolo, entonces, será seguro si la distribución y asignación de claves públicas es un proceso seguro.

* **Centro de Distribución de Claves (KDC):** Es la única entidad que proporciona los valores de claves compartidas o simétricas para comunicarse con todas las entidades de la red. Además el KDC conoce la clave secreta de cada usuario registrado y el usuario puede comunicarse con el KDC a través de esa clave.
* **Autoridad de Certificación (CA):** Autoridad que certifica si una clave pública pertenece a una entidad en específico. Estas claves son públicas en alguna parte, como una página de Internet, para que un usuario pueda comunicarse con el dueño de la clave.

**Conclusiones**

* La seguridad en Internet es un tema de constante preocupación y cambio con el fin de mantener protegida la información confidencial que se comparte entre algunos usuarios de Internet. Existen diversas formas actualmente de mantener una transferencia de datos de forma segura y privada, no obstante, los ataques cibernéticos son cada vez más sofisticados, por lo que se debe renovar constantemente.
* Las técnicas actuales permiten la comprobación exacta de la identidad del receptor de la información privada a enviar. Este tipo de seguridad es muy útil en transferencias bancarias, Universidades, empresas, etc.
* La tecnología está en constante cambio a medida que los requerimientos por parte de los usuarios aumenta, por lo que esta área siempre requerirá un grupo de ingenieros dedicados a la investigación.

**Referencias**

James F. Kurose and Keith W. Ross, *"Computer Networking: A top-Down Approach Featuring the Internet"*, Addison Wesley, Third Edition 2005