Universidad de Costa Rica

Escuela de Ciencias de la Computación e Informática

Redes de Comunicación de Datos

CI-0121

Grupo 002

Seguridad en Redes

Profesor:
José Antonio Brenes Carranza

Autores:

Diego Madrigal Salazar

Reichel Mora Villegas

María Peraza Durán

José Ignacio Víquez Rojas

24 de septiembre de 2020

Índice

1. Introducción

En la actualidad un tema de gran importancia debido al crecimiento en el tema de redes de comunicación de datos, sin duda alguna es la seguridad informática, el cual podemos definir según la Universidad Internacional de Valencia (s.f.) como el proceso de prevenir y detectar el uso no autorizado a un sistema informáticos, esto implica el proceso de protegernos contra intrusos el uso de nuestros recursos informáticos con malas intenciones, entre ellas, obtener ganancias, fraudes, robos, acceso a información confidencial, etc.

Las cuatro áreas principales que cubre la seguridad informática son las siguientes:

- **Confidencialidad:** Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
- **Integridad:** Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
- **Disponibilidad:** Los datos deben estar disponibles para los usuarios cuando sea necesario.
- **Autenticación:** Estás realmente comunicándote con los que piensas que te estás comunicando.

El objetivo de esta investigación consiste en el análisis de diferentes mecanismos, tecnologías o medidas de seguridad utilizadas con el fin de preservar la integridad de nuestros datos en las redes a partir de los cuatros puntos mencionados anteriormente. Entre ellos se destacan la criptografía, las llaves públicas y privadas, las redes privadas virtuales (VPN), las redes MLPS, entre otros que se tratarán a lo largo del desarrollo de este trabajo.

2. Seguridad en Redes

2.1. Criptografía

La criptografía comprende una serie de técnicas de cifrado y descifrado utilizadas con el fin de proteger documentos y datos de diferente índole o desde otro punto de vista para lograr el intercambio de mensajes y que estos solamente puedan ser leídos e interpretados por su receptor. El término proviene del griego kryptos cuyo significado es “ocultar” y de grafos que significa “escritura”, por lo que criptografía significa “escritura oculta”.

Tanenbaum (2013) afirma que en la historia, la criptografía ha sido mayormente utilizada por cuatro grandes grupos: los militares, el cuerpo diplomático, los periodistas y los amantes, y de estos grupos el que ha dominado aún más el campo es la milicia. Un caso que destaca en este campo, se presentó en la II Guerra Mundial, en donde Alemania había conseguido dominar el Atlántico Norte con su flota de submarinos, y sus comunicaciones eran indescifrables gracias a la máquina Enigma, que se le atribuye a Alan Turing.

En el campo de las redes, Venturini (2020) afirma que la criptografía funciona a través de la implementación de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Con el desarrollo de las computadoras, la criptografía se ha extendido, utilizado y modificado ampliamente tanto que se llegó a constituir por medio de algoritmos matemáticos.

Actualmente este mecanismo es usado en muchas áreas de lo que comprende redes, como por ejemplo el tema de la seguridad de las comunicaciones mediante el establecimiento de canales seguros, en donde se asegure la privacidad sin perder velocidad de transmisión, otra aplicación la autenticación de usuarios, dado que surge la gran necesidad de demostrar que somos quien decimos ser y además de que el receptor es quien dice ser. Es posible su aplicación en un campo que se encuentra en gran auge: en el comercio electrónico, dado que la criptografía establece diferentes canales seguros y métodos de identificación asegurando que tanto los usuarios que desean comprar y las empresas que ofrecen sus productos estén seguros de situaciones como robos, fraudes, etc.

Sin duda alguna otro uno de los grandes usos de la criptografía se encuentra en Internet, por ejemplo los sitios que son HTTPS, poseen un protocolo denominado SSL, que básicamente se encarga de cifrar la comunicación que existe entre el cliente y el servidor, evitando que terceros puedan interceptar comunicaciones y con esto obtener datos sensibles o confidenciales, que eventualmente pueden conducir a situaciones como robos, fraudes, etc, un ejemplo claro es de los sitios que se especializan en la venta de productos, y los usuarios deben colocar sus datos bancarios para realizar una compra. De igual manera, este cifrado protege datos de acceso, correos, nombres y mucho más. (León, 2019). Otro de los ejemplos es el cifrado de DNS, según Wu (2019) este mecanismo hace que sea más difícil espiar los mensajes de DNS o que los mismos sufran alteraciones mientras están en tránsito; existen dos mecanismos estandarizados relativamente nuevos para garantizar que el traslado de DNS entre el receptor y el resulutor, DNS mediante TLS (2016) y consultas de DNS mediante DNS mediante HTTPS (2018). Estos mecanismos se basan en la seguridad de la capa de transporte (TLS, del término en inglés Transport Layer Security), la misma que se utiliza para la protección entre el usuario y los sitios web que utilizan HTTPS; en dicha capa, el servidor (ya sea un servidor web o un resolutor de DNS) utiliza un certificado para autenticarse automáticamente en el dispositivo del cliente, esto asegura que ninguna otra parte pueda hacerse pasar por el servidor (Wu, 2019).

Ahora bien, que se mencionó el tema bancario, sin duda si existe una área donde es de suma importancia la aplicación de la criptografía es el ámbito de los sistemas financieros en donde es vital es resguardo de toda la información que se maneja en dichas plataformas, acá en cuanto al protocolo o tecnología utilizada, podemos mencionar hash, WTLS, SSL, etc. Sin mencionar que muchas de estas instituciones también utilizan sus propios mecanismos de seguridad para garantizar una mayor seguridad en sus plataformas virtuales (León, 2019).

La criptografía cumple un gran papel en el área de los correos electrónicos, medio que sigue siendo de gran importancia para muchas personas. Por ejemplo, según León (2019) S-MIME es un mecanismo que se encarga de cifrar todos los correos enviados desde una plataforma de correo; de esta manera, se evita que terceros puedan tener acceso al contenido confidencial de estos correos, sin embargo según Rabenstein (2020) solamente el contenido del correo electrónico está cifrado, pero no los metadatos, por lo que la información como el remitente, el destinario o el asunto del mensaje sigue siendo legible. Por otra parte, este sistema también otorga seguridad al momento de autenticar, integrar y no repudiar a un usuario de la plataforma de correo en cuestión. Además algunas plataformas de correo electrónico hacen uso de los mecanismos de cifrado de transporte mencionados con anterioridad, entre ellos SSL y TLS (Rabenstein, 2020).

Sin duda alguna la criptografía juega un papel sumamente importante en todo lo que concierne a las redes de comunicación de datos, por lo que en las siguientes secciones se profundiza en estos mecanismos y sus diferentes tipos y algoritmos.

2.1.1. Criptografía Simétrica

Según Tech Blog (2020) este tipo de cifrado se ocupa de la clave única entre el remitente y el receptor. Es decir, ambos extremos de la comunicación conocen de antemano la clave o contraseña, porque previamente fue compartida a través de un canal sin filtros ni protocolos, como llamadas telefónicas; correo; una hoja de papel; una hoja de papel, etc. Es en este punto que su mayor vulnerabilidad radica en esto: el canal envía la clave de la misma manera que la clave recibida; es muy fácil interceptar el canal para interceptar la clave y encontrar todos sus componentes sin romper el código.

Figura 1: Criptografía Simétrica

La principal ventaja que ofrece la criptografía simétrica es la velocidad de creación y entrega de mensajes. Sin embargo, si nuestro objetivo es proteger y privatizar la información que compartimos, su extrema vulnerabilidad la hace poco confiable y no recomendada en absoluto.

2.1.2. Criptografía Asimétrica

A diferencia de la anterior, la criptografía asimétrica utiliza dos claves para hacer que los mensajes sean más robustos y difíciles de entender. Una de estas claves es pública y por lo tanto no proporciona una barrera de protección porque su único propósito es establecer un canal (o receptor) para reenviar o entregar mensajes. La otra clave es la clave privada. Ella es responsable de cifrar los mensajes para mantenerlos privados. Este par de claves se genera al mismo tiempo, y el propietario decide a quién revelarlo. (TechBlog, 2020).

Figura 2: Criptografía Asimétrica

La solidez de una clave asimétrica depende principalmente del tamaño del código de cifrado, que puede alcanzar fácilmente los 2048 bits. Además, cada intento de descifrar el código se vuelve

más difícil, sin embargo este tipo de cifrado presenta la desventaja de la lentitud con la que se verifican los datos.

2.1.3. Criptografía Híbrida

Según Gutiérrez (2017), este sistema es una combinación de las dos tipos anteriores. Se debe asumir que los problemas de los dos criptosistemas son la inseguridad simétrica y la velocidad lenta asimétrica. El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo):

- Generar una clave pública y otra privada (en el receptor).
- Cifrar un archivo de forma síncrona.
- El receptor nos envía su clave pública.
- Ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor.
- Enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).

Figura 3: Criptografía Híbrida

2.2. Llave pública y privada

A lo largo de la historia siempre se ha existido un problema de cómo se deben distribuir las claves, sin importar lo importante que sea dicha llave, si un intruso encuentra la forma de obtenerla ocasionaría que el sistema quede inservible.

Se propone, entonces una clase totalmente nueva de criptosistema, uno en donde las claves de encriptación y desencriptación eran tan diferentes que no era posible derivar una a partir de la otra. En dicho criptosistema, se definen tres principios como se menciona en Tanenbaum (2013), para los cuales declaramos a “E” como el algoritmo de encriptación y a “D” como el algoritmo de desencriptación. Tanto E como D deben de cumplir con lo siguiente:

- D (E(P)) = P.
- Es demasiado difícil deducir D a partir de E.
- E no se puede descifrar mediante un ataque de texto plano elegido.

El primer requerimiento especifica que si se aplica D a un mensaje cifrado “E(P)” entonces se obtiene el mensaje original “P”. Si no se tuviera este requerimiento el receptor legítimo no podría desencriptar el texto cifrado. Con respecto al tercer requerimiento, es para evitar que cualquier intruso se infiltre a cambiar partes del algoritmo. Si se cumplen estas tres condiciones, no hay razón para que una clave de encriptación no se pueda hacer pública, ya que como vimos en el segundo requerimiento, es casi imposible encontrar “D” a partir de “E”.

Figura 4: Funcionamiento de claves.

Entonces ¿que es una llave pública y una privada ? Bueno una llave publica es la clave que usa el usuario para encriptar los mensajes desee enviar a otro y una llave privada que es la clave con la que el usuario descripta el mensaje. Podemos decir que cada usuario requiere entonces de dos llaves una privada y una pública para enviar mensajes. Antes de continuar es importante comentar, como aparece en González Rodríguez, M. González Rodríguez, M. (Ed.) y Stallings, W. (2004, pag: 71) :

> “.. la seguridad de cualquier esquema de cifrado depende (1) la longitud de la clave y (2)del coste computacional necesario para romper el cifrado.”

Se necesita encontrar algoritmos que satisfagan las condiciones mencionadas. El algoritmo más usado es el denominado RSA(Rivest, Shamir, Adleman), su única desventaja es que requiere de llaves de por lo menos 1024 bits para una buena seguridad, por lo cual es muy lento .Según Tanenbaum (2013): este algoritmo se basa en:

1. Seleccionar dos números primos grandes, p y q (por lo general de 1024 bits).
2. Calcular n = p * q y z = (p - 1) * (q - 1).
3. Seleccionar un número que sea relativamente primo para z y llamarlo d.
4. Encontrar e de tal forma que e * d = 1 mod z

Veamos un ejemplo, tomado de Tanenbaum (2013):

“ ...Para este ejemplo hemos seleccionado p =3 y q= 11, lo cual nos da n = 33 y z = 20. Un valor adecuado para d es d = 7, puesto que 7 y 20 no tienen factores comunes, con base en estas opciones,podemos encontrar a e si resolvemos la ecuación :

$$7e = 1(mod 20) \tag{1}$$

Que da como resultado $e = 3$. El texto cifrado C, que corresponde a un mensaje de texto plano P, se obtiene mediante:

$$C = P^3(mod 33) \tag{2}$$

El receptor desencripta el texto cifrado mediante la regla:

$$P = C^7(mod 33) \tag{3}$$

En la figura se muestra como ejemplo la encriptación del texto plano “SUZANNE”.”

Texto plano (P)			Texto cifrado (C)		Después de la desencriptación	
Simbólico	Numérico	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Simbólico
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
		Cálculo del emisor		Cálculo del receptor		

Figura 5: Ejemplo RSA. Fuente: Tanenbaum(2013)

Como se menciona en González Rodríguez, M. González Rodríguez, M. (Ed.) y Stallings, W. (2004), los valores de n y e deben ser conocidos por ambos pero solo el receptor deber conocer el valor de d. Como nota adicional es importante saber que el RSA es demasiado lento para poder encriptar grandes volúmenes de datos, pero se utiliza mucho para distribuir las claves.

2.2.1. Firmas digitales

Para poder sustituir los papeles firmados a una manera digital es necesario desarrollar una manera de comprobar documentos de manera imposible de falsificar. Lo anterior no es un asunto tan sencillo ya que se ocupa que se cumplan las siguientes condiciones :

- Que el receptor pueda verificar la identidad del emisor.
- Que el emisor no pueda negar más tarde el contenido del mensaje.
- Que el receptor no haya podido falsificar el mensaje él mismo.

Firma de clave simétrica

Una metodología para las firmas digitales es tener una autoridad central que sepa todo y en quien todos confíen, digamos BB. Cada usuario escoge una clave secreta y la lleva personalmente a

las oficinas del BB, así solo el usuario y el BB conocen la clave secreta. A continuación se presenta una explicación tomada de Tanenbaum (2013):

> " Alice y el BB conocen la clave secreta de Alice,KA, y así sucesivamente. Cuando Alice desea enviar un mensaje de texto plano firmado (P) a su banquero Bob, genera KA(B,RA, t, P), en donde B es la identidad de Bob, RA es un número aleatorio elegido por Alice, t es una estampa de tiempo para asegurar que el mensaje sea reciente, y KA(B, RA, t, P) es el mensaje encriptado con su clave, KA. El BB ve que el mensaje proviene de Alice, lo descripta y envía un mensaje a Bob. El mensaje para Bob contiene el texto plano del mensaje de Alice y también el mensaje firmado KBB(A, t, P). Ahora, Bob se encarga de la solicitud de Alice. "

Y ¿si Alice dice no haber enviado el mensaje ? Bob puede asegurar que el mensaje fue validado por el BB o sea este viene de con KA, y como Bob tiene KBB (A, t, P) y además el BB, que recordemos es una entidad de confianza, puede desencriptar el mensaje con lo que la firma es verdadera. Además es importante mencionar que no se pueden dar replicaciones de documentos ya que cada envío posee una marca de tiempo que indica el momento en el que fue mandado.

Firma de clave pública

Un problema que se da al trabajar con la criptografía de clave simétrica para firmas digitales es que todos tienen que confiar en el BB (autoridad central) y muchas veces este no es el caso; entonces seria bueno si la firma no requiriera de una autoridad de confianza o un tercero. Por fortuna podemos usar la criptografía de llave publica en este caso. Vamos a suponer que los algoritmos de encriptación y desencriptación de clave pública tienen la propiedad de que $E(D(P)) = P$, además de la propiedad normal de que $D(E(P)) = P$.

Veamos este escenario planteado en el libro de texto de Tanenbaum (2013) :

> "Alice puede enviar un mensaje de texto plano firmado (P) a Bob al transmitir EB(DA(P)). Observe bien que Alice conoce su propia clave (privada), DA, así como la clave pública de Bob, EB, por lo que Alice puede elaborar este mensaje. Cuando Bob recibe el mensaje, lo transforma mediante su clave privada de la manera usual, para producir DA(P) como se muestra en la figura "ejemplo firma clave publica". Bob almacena este texto en un lugar seguro y después aplica EA para obtener el texto plano original. Para ver cómo funciona la propiedad de firma, suponga que más tarde Alice niega haber enviado el mensaje P a Bob. Cuando el caso llega a la corte, Bob puede presentar tanto P como DA(P). El juez puede comprobar fácilmente que Bob tiene un mensaje válido encriptado por DA con sólo aplicarle EA. Puesto que Bob no conoce la clave privada de Alice, la única forma en que Bob pudo haber adquirido un mensaje encriptado por esa clave sería que Alice en efecto lo hubiera enviado. "

Existen dos problemas usando la firma de clave pública. El primero es que Bob podría demostrar que fue Alice la que le envio el mensaje siempre y cuando DA permanezca privado, si Alice decide liberarla no hay manera de demostrar quien envió el mensaje. El otro problema surge si Alice decide cambiar su clave ya que entonces no podría ser descifrado y Alice tiene todo el derecho de cambiar su clave.

Resúmenes de mensajes

Si lo que se busca es autenticación pero no confidencialidad se usa un sistema que no encripta

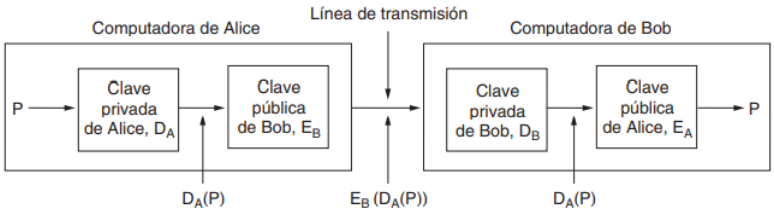

Figura 6: Ejemplo firma clave pública. Fuente: Tanenbaum(2013)

todo el mensaje. Este esquema se basa en la idea de una función de hash unidireccional que toma una parte arbitrariamente grande de texto plano y calcula una cadena de bits de longitud fija. Esta función de hash, MD, que se conoce comúnmente como resumen de mensaje (message digest). Este esquema tiene propiedades importantes, según lo que se plantea en Tanenbaum (2013) :

1. Dado P, es fácil calcular MD(P).
2. Dado MD(P), es en efecto imposible encontrar P.
3. Dado P, nadie puede encontrar P' de tal manera que MD(P') = MD(P). Lo que se conoce como unidireccional.
4. Un cambio en la entrada de incluso 1 bit produce una salida muy diferente

Para cumplir con el punto 3 se ocupa que la función hash sea de al menos 128 bits de longitud y para cumplir con el criterio 4 la función hash debe de truncar los bits de manera minuciosa. Según se explica en González Rodríguez, M. González Rodríguez, M. (Ed.) y Stallings, W. (2004, pag: 62):

> "... un resumen de mensaje también proporciona integridad de los datos."

Esto ya que si algún bit del mensaje se altera en el intercambio el mensaje resultante del resumen sera erróneo.

Vale la pena saber que es mucho mas rápido calcular el resumen del mensaje de una pieza de texto que encriptarlo usando algún algoritmo de llave publica. Para explicar como funciona, recordemos el ejemplo del BB para una firma de clave publica.Imaginemos un escenario donde Alice quiere enviar un mensaje a Bob sin el BB. Si Alice quisiera enviar un mensaje primero debería de calcular el resumen de mensaje mediante la aplicación de MD al mensaje P y esto produce MD(P). Seguidamente Alice incluye KA(A,t,MD(P), P) y lo envía al receptor, Si ocurriera una disputa como en los ejemplos mostrados anteriormente dado que es prácticamente imposible que el receptor encuentre otro mensaje que de este resultado de la función hash, se le deberá dar la razón al receptor.

Al usarlos resúmenes de mensaje de esta manera, obtenemos un ahorro tanto en el tiempo de encriptación como en los costos de transporte de los mensajes.

Los resúmenes de mensaje se pueden usar también en los criptosistemas de clave publica. Podemos ver un ejemplo en la imagen "Firmas digitales mediante el uso de MD".

Existen variedad de funciones para el resumen de mensajes, a continuación explicaremos una de las mas usadas SHA-1(Algoritmo de hash seguro 1), básicamente todos los resúmenes de mensajes que se basan en un hash usan los mismos principios, Se tiene una entrada que se va a dividir en secuencias de bloques de bits, esta entrada se va trabajando bloque a bloque para producir una

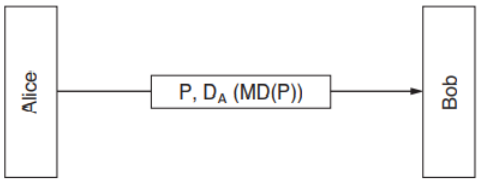

Figura 7: Firmas digitales mediante el uso de MD. Fuente: Tanenbaum(2013)

salida de n bits transformada por la función hash.SHA-1 procesa los datos de entrada en bloques de 512 bits y genera un resumen de 160 bits. La figura Üso de SHA-1"muestra una comunicación de un mensaje no secreto. Podemos ver como se genera un hash usando el algoritmo SHA-1 y después se firma usando el RSA. La explicación de como funciona RSA es la dada por Tanenbaum (2013, p.690-691) :

> " Empieza por rellenar el mensaje al agregar 1 bit al final, seguido de tantos bits 0 como sean necesarios (pero como mínimo 64) para que la longitud sea un múltiplo de 512 bits. A continuación, al número de 64 bits que contiene la longitud del mensaje antes del relleno se le aplica un OR en los 64 bits de menor orden. En la figura .Explicación SHA-1", el mensaje se muestra con un relleno a la derecha debido a que el texto y las figuras van de izquierda a derecha (es decir, por lo general el extremo inferior derecho se percibe como el final de la figura). Durante el cálculo, SHA-1 mantiene cinco variables de 32 bits, H0 a H4, donde se acumula el hash. Dichas variables se muestran en la figura 8-22(b). Se inicializan con constantes especificadas en el estándar.Ahora se procesa cada uno de los bloques M0 a M n1. Para el bloque actual, las 16 palabras primero se copian al inicio de un arreglo auxiliar de 80 palabras, W, como se muestra en la figura 8-22(c). Después las otras 64 palabras de W se rellenan mediante la fórmula:

$$Wi = S1(W_{i-3}\ XOR\ W_{i-8}\ XOR\ W_{i-14}\ XOR\ W_{i-16}) \qquad (16 \leq i \leq 79) \qquad (4)$$

> en donde Sb(W) representa la rotación circular izquierda de la palabra de 32 bits, W, por b bits. Ahora cinco variables de trabajo A a E se inicializan desde H0 hasta H4, respectivamente. Podemos expresar el cálculo real en pseudo-C de la siguiente forma:

```
for (i = 0; i < 80; i++) {
    temp = S5(A) + fi(B,C,D) + E + Wi + Ki;
    E = D; D = C; C = S30(B); B = A; A = temp;
}
```

> en donde las constantes Ki se definen en el estándar. Las funciones de mezcla fi se definen como:

$$fi(B,C,D) = (B\ \ AND\ \ C)\ \ OR\ \ (NOT\ \ B\ \ AND\ \ D) \quad (0 \leq i \leq 19) \qquad (5)$$

$$fi(B,C,D) = B\ \ XOR\ \ C\ \ XOR\ \ D \quad (20 \leq i \leq 39) \qquad (6)$$

$$fi(B,C,D) = (B\ \ AND\ \ C)\ \ OR\ \ (B\ \ AND\ \ D)\ \ OR\ \ (C\ \ AND\ \ D)\ \ (40 \leq i \leq 59) \qquad (7)$$

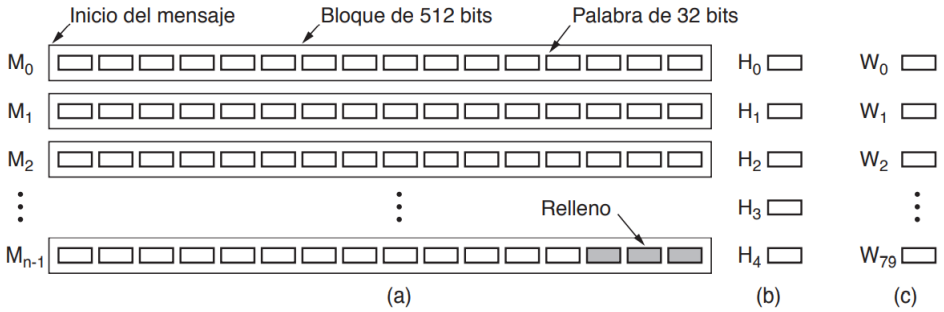

Figura 8: Explicacón SHA-1. Fuente: Tanenbaum(2013)

$$fi(B,C,D) = B \;\; XOR \;\; C \;\; XOR \;\; D \quad (60 \leq i \leq 79) \tag{8}$$

Cuando se completan las 80 iteraciones del ciclo, las variables A a E se agregan a las variables H0 a H4,respectivamente. Ahora que se ha procesado el primer bloque de 512 bits, se inicia el siguiente. El arreglo W se reinicia desde el nuevo bloque, pero H se deja como estaba. Al terminar este bloque se inicia el siguiente, y así en lo sucesivo hasta que todos los bloques de mensajes de 512 bits se hayan procesado por completo. Al terminar el último bloque, las cinco palabras de 32 bits en el arreglo H se envían a la salida como el hash criptográfico de 160 bits. El código de C completo para SHA-1 se proporciona en el RFC 3174. ”

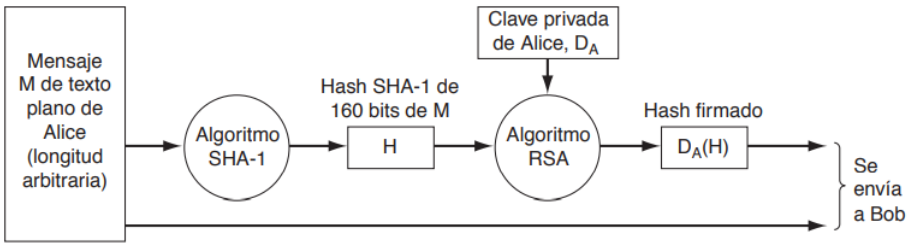

Figura 9: Uso de SHA-1. Fuente: Tanenbaum(2013)

2.2.2. Administración de claves públicas.

Mediante los temas que se han tratado en la sección anterior(clave pública, firmas de mensajes sin terceros y resúmenes de mensajes firmados) el receptor puede verificar los mensajes que le llegan. Pero si las dos personas que realizan el intercambio no se conocen ¿cómo obtienen la llave pública del otro para comenzar la comunicación ? Se podría pensar que al ponerla en una pagina web este problema desaparece ya que las personas interesadas podrían conseguir la llave fácilmente, pero pensar de esta manera seria un error ya que podría existir un tercero que intercepte la señal y sustituya la clave con el fin de que los mensajes le lleguen primero a el y no al receptor original. Con lo anterior es obvio que es necesario un mecanismo para asegurar claves publicas, es por esto

que existen los certificados.

Certificados

Como se explica en González Rodríguez, M. González Rodríguez, M. (Ed.) y Stallings, W. (2004, pag: 82) :

> " ... un certificado consiste en una clave pública y un identificador o nombre de usuario del dueño de la clave, con todo firmado por una tercera parte confiable."

A una organización que certifica claves públicas se le conoce como CA(Certificate Authority). El trabajo fundamental de un certificado es enlazar una clave pública con el nombre de un personaje principal. Es de suma importancia aclarar que los certificados no son secretos ni están protegidos ya que mas bien estos existen para validar la identidad de una persona o organismo. Si se tuviera un único centro de distribución de llaves publicas este podría convertirse en un cuello de botella, además tendría la limitante de solo funcionar por medio de internet.

Si una persona interesada quisiera contactar a otra y quisiera corroborar que el certificado corresponde al de la persona con la que se quiere comunicar, esta persona podría realizar el algoritmo de SHA-1 sobre el certificado y si obtiene un hash que no corresponde sabrá que la información de la clave no es segura, lo que quiere decir que esta clave no corresponde a la persona con la que desea comunicarse.

Los certificados también pueden ser usados para enlazar una clave a un atributo. Esto es útil cuando se quiere acceder a cierto material pero no se quiere revelar la identidad del dueño.

Si todas las personas acudieran a la CA a obtener algo firmado con un tipo diferente de certificación distinta la administración seria un caos. Para que no pase esto se diseñaron estándares para los certificados aprobados por la ITU (International Telecommunication Union), ese estándar se conoce como X.509 y se utiliza mucho en internet. Básicamente, el X.509 es una forma de describir certificados, cada espacio del certificado aparece en la imagen "Campos de un certificado X.509". Por ejemplo, si Juan trabaja en el Departamento de Carreteras de la Empresa Constructora JJ, su dirección X.500 podría ser: /C=MX/O=Empresa Constructora JJ/OU=Carreteras/CN=Juan/ Donde: C corresponde al país, O a la organización, OU a la unidad organizacional y CN a un nombre común. Un problema que se podría dar es que si en el mismo departamento existiera mas de una persona llamada Juan no se podría identificar.

Campo	Significado
Versión	Qué versión de X.509.
Número de serie	Este número más el nombre de la CA identifican el certificado de manera única.
Algoritmo de firma	El algoritmo utilizado para firmar el certificado.
Emisor	El nombre X.500 de la CA.
Periodo de validez	Los tiempos inicial y final del periodo de validez.
Nombre del sujeto	La entidad cuya clave se va a certificar.
Clave pública	La clave pública del sujeto y la ID del algoritmo que la utiliza.
ID del emisor	Un ID opcional que identifica al emisor del certificado en forma única.
ID del sujeto	Un ID opcional que identifica al sujeto del certificado en forma única.
Extensiones	Se han definido muchas extensiones.
Firma	La firma del certificado (firmada por la clave privada de la CA).

Figura 10: Campos de un certificado X.509. Fuente: Tanenbaum(2013)

Infraestructura de clave pública

No puede existir una sola CA que emita todos los certificados del mundo si fuera una sola compañía con varias sucursales esto daría pie a fuga de claves. Por estas razones se ha desarrollado una forma diferente para certificar claves públicas. Su nombre general es PKI (Infraestructura de Clave Pública). Una PKI tiene varios componentes como: usuarios, autoridades certificadoras (CA) , certificados y directorios. La PKI se encarga de proporcionar una forma de estructurar estos componente y definir estándares, podemos ver a una PKI como una jerarquía de autoridades CA.

La CA de mayor nivel certifica a las autoridades CA de segundo nivel (RA: Autoridades Regionales) y viceversa.

El siguiente ejemplo brindado por Tanenbaum (2013, p. 698):

> " Suponga que Alice necesita la clave pública de Bob para comunicarse con él, por lo que busca y encuentra un certificado que la contenga, firmado por la CA 5. Sin embargo, Alice nunca ha escuchado acerca de la CA 5. En lo que a ella respecta, la CA 5 podría ser la hija de 10 años de Bob. Podría ir con la CA 5 y decirle: "Prueba tu autenticidad". La CA 5 le responderá con el certificado que obtuvo de la RA 2, el cual contiene la clave pública de la CA 5. Una vez que tenga la clave pública de la CA 5, Alice podrá verificar que el certificado de Bob realmente fue firmado por la CA 5 y que, por lo tanto, es legal. "

Ahora nos puede surgir la duda ¿Y cómo averigua Alice la clave pública de la raíz?. No es necesario que lo averigüe ya que se supone que todos la conocemos. Por ejemplo, su navegador podría tener integrada la clave pública de la raíz.

Directorios

Los directorios son donde se almacenan los certificados generados por una PKI. Hay dos opciones que cada usuario guarde la propia, que genera inconvenientes y almacenarlos en una DNS (The Domain Name System (DNS) es la "guía telefónica"de internet.)

Revocación

Existen ocasiones en las que se deben de remover certificados. Una razón para esto seria que la llave privada de la CA ha sido comprometida. Para poder manejar estas situaciones existen la CRL (Lista de Revocación de Certificados) que proporciona los números de los certificados que han sido removidos. Es importante mencionar en este punto que los certificados tienen tiempo de expiración y cuando este vence se invalida de manera automática. Existe sin embargo un problema con esta practica según dice Tanenbaum (2013, pag: 699):

> " Por desgracia, introducir listas CRL significa que un usuario que está próximo a utilizar un certificado debe adquirir la CRL para ver si éste se revocó. Si es así, dicho certificado no debe utilizarse. Sin embargo, si el certificado no está en la lista, pudo haber sido revocado justo después de que se publicó la lista. Por lo tanto, la única manera de estar seguro realmente es preguntar a la CA. Y la siguiente vez que se utilice ese mismo certificado, se le tiene que preguntar de nuevo a la CA, puesto que pudo haber sido revocado segundos antes. Otra complicación es que un certificado revocado puede reinstalarse nuevamente; por ejemplo, si se revocó por no pagar una cuota que ya se encuentra al corriente. Al tener que lidiar con la revocación (y quizá

con la reinstalación), se elimina una de la mejores propiedades de los certificados; es decir, que pueden utilizarse sin tener que contactar a una CA."

Ahora ¿dónde se almacena esta lista CRL? Una buena estrategia sería en el mismo directorio en donde están los certificados o en la cache de ciertos sitios de internet.

2.3. Seguridad de la Comunicación

Es importante asegurar que los paquetes que se envían a través de la red lleguen sin ninguna alteración y de manera segura desde su origen hasta el final de su recorrido. Para ello existen herramientas como las Redes Privadas Virtuales, IPsec, los firewalls y la estrategia de tunneling las cuales se analizarán más detalladamente a continuación.

2.3.1. Redes privadas virtuales (VPN)

Una red privada se refiere a una red a la que únicamente pueden tener acceso ciertas computadoras y líneas telefónicas de una organización determinada. Para 1983 se da la aparición de internet, donde Tanebaum (2013, pag 706) afirma que esto provocó que muchas empresas desearan cambiar sus servicios a la red pública, sin embargo, querían mantener la seguridad que brindaba la red privada. Esto dio paso a la creación de las redes privadas virtuales (VPN), las cuales son redes privadas que se encuentran superpuestas sobre redes públicas pero que mantienen ciertas características de las redes privadas, como la seguridad, lo cual permite establecer una conexión a través de un medio seguro y confiable.

Otra estrategia que se puede utilizar es hacer que el ISP establezca la VPN a través del uso de MPLS (Multiprotocol Label Switching) donde "se pueden establecer las rutas para el tráfico de la VPN a través de la red del ISP entre las oficinas de la empresa."(Tanebaum, 2013, pag 707) lo que hace que el tráfico del VPN y el del internet estén separados.

Diaz, Alzorriz y Sancristobal(2014, pag 489) mencionan que algunos de los usos principales que se da al internet actualmente pueden ser:

- Intranet: generalmente las comunicaciones que se llevan a cabo son de red a red y se utiliza para conectar redes físicas de una organización que posee varias sedes en zonas distantes geográficamente haciendo uso de una VPN que se encuentra construida sobre Internet.
- Extranet: es bastante similar a la anterior, pero difiere sobre todo en lo que respecta a quienes pueden acceder a ella ya que en intranet solo se permite el acceso de los integrantes de la propia organización en cambio en la extranet distintas compañías, clientes, socios y demás pueden tener acceso a la red.
- Acceso remoto: brinda acceso a la red a personas que trabajan desde sus hogares o a los que están constantemente cambiado de ubicación.

Vacca (2013) comenta que en un principio eran mayormente utilizadas por compañías grandes sin embargo ahora se han convertido en parte de empresas más pequeñas las cuales la utilizan como una forma de permitir que los usuarios remotos accedan a sus sitios comerciales. Esta red posee la capacidad de enrutar las comunicaciones por medio de una red pública que da permiso de

accedo a ciertos servidores

Otra acotación que realiza Vacca(2013,pag 511) es que las empresas que utilizaban esta clase de tecnología tenían como objetivo conectar distintas zonas a sistemas informáticos remoto. Esta clase configuración logró que la comunicación entre sitios fuera segura con lo cual se permite acceder a fuentes informáticas y sistemas de comunicación de forma segura. Muchos de los sitios eran muy costosos para acceder a ellos sin embargo con la llegada del VPN la posibilidad de tener acceso a ellos es mucho mayor.

Existen varias organizaciones que trabajan en los entandares en cuanto a las redes de computadoras así como empresas privadas que se organizan en la creación de nuevos protocolos para mejorar los servicios de las VPN, dos de ellos son Internet Engineering Task Force y el Institute of Electrical and Electronic Engineers(IEEE).

2.3.2. IPsec

Ipsec hace referencia a un protocolo de seguridad para la capa de red donde se brinda seguridad a los datagramas que son intercambiados por dos entidades dando servicios que utilizan criptografía de clave simétrica. Kurose y Ross (2010, pag 700) indican que entre las dos entidades que se van a transmitir paquetes se establece una conexión lógica llamada asociación de seguridad la cual se refiere a una conexión entre un origen y un destino la cual cuenta con un id de seguridad. Entre las principales características de seguridad que da IPsec están la integridad de datos, la autenticación, privacidad de los datos que serán transmitidos y la protección contra las repeticiones de mensajes.

Tanebaum (2013, pag 701) menciona otro protocolo que forma parte del Ipsec llamado IKE(Internet Key Exchange) encargado de establecer las llaves así como los dos modos en que puede trabajar: el modo de transporte y el modo túnel. El modo de transporte, que según Gonzalez, Gonzales y Stallings(2004, pag 199) da protección principalmente a las capas superiores, se utiliza generalmente para la comunicación extremo a extremo entre hosts y el modo túnel en su lugar brinda protección todo el paquete IP.

Este protocolo cuenta con dos encabezados principales:

- AH (Authentication Header): este proporciona verificación de integridad (comprobar que la información no ha sido modificada en el transcurso de su transporte) así como autenticación (se puede determinar quien envió la información) sin embargo no posee protección sobre la confidencialidad ya que no hay encriptación de datos. Tanebaum (2013, pag 702) menciona las diferentes partes por las cuales está compuesto un encabezado: el siguiente encabezado que posee el dato que se encontraba en el espacio del protocolo de IP, la longitud de carga útil que se refiere al número de palabras en el encabezado AH menos dos, el índice de parámetros de seguridad el cual es un id para la conexión, el número de secuencia cuyo principal uso es para detectar ataques de repetición ya que cada paquete posee un número de paquete único y por último los datos de autenticación que almacena la firma digital.

- ESP (Encapsulation Security Payload): este otro encabezado, al igual que el AH, brinda verificación de integridad, autenticación pero también confidencialidad. Ya que este último

aspecto es fundamental para aplicaciones IPsec, Kurose y Ross (2010, pag 727) afirman que ESP es mucho más usado que el encabezado AH. Las partes que conforman a ESP son un campo de índice de parámetros de seguridad y número de secuencia (se presenta en AH), vector de inicialización el cual es para encriptar los datos y verificaciones de identidad.

2.3.3. Firewalls

Tanebaum (2013, 704) compara los firewalls o cortafuegos con los pozos que se construían alrededor de un castillo, cuya función era que las personas que quisieran llegar al castillo solo podrían acceder a él través de un puente. Esto mismo hacen los firewalls haciendo que los paquetes que se transportan solo puedan pasar a través de un único medio.

Este sistema de seguridad se encarga de examinar todos los paquetes que le llegan y los que salen, así como buscar los paquetes que no han sido autorizados que están intentando acceder a la red. Su objetivo principal es evitar que ingresen usuarios no deseados, así como evitar que información clasificada sea filtrada. Vacca (2013, pag 159) menciona que el bloquear el tráfico no deseado, dirigir el tráfico entrante a nodos internos más confiables y registrar el tráfico que va hacia y desde la red son algunos de los tipos de seguridad que nos brinda el uso de firewalls.

Los firewalls se pueden encontrar de varias formas. Tanebaum (2013, 704) menciona tanto los firewalls con estado como los que utilizan puertas de enlace a nivel de aplicación. Los firewalls con estado se refieren a paquetes que se asocian a conexiones y que utilizan espacio del encabezado para llevar un registro de las conexiones mientras que los que utilizan puertos de enlace realizan un análisis más profundo de los paquetes donde puede ver lo que está realizando la aplicación.

Generalmente se pueden encontrar 4 tipos de firewalls: los filtros de paquetes, los gateways de aplicaciones, los stateful inspection y los híbridos. Los filtros de paquetes se ubican entre la red que se está intentando proteger y todo lo demás y su función principal es filtrar el tráfico a través de las combinaciones de las cabeceras. Sin embargo Abad(2013, 240) menciona que el hecho de que este sea tan sencillo puede provocar que a la hora de implementar filtros que posean una mayor dificultad sea más complicado de llevar a cabo. Los gateways de aplicaciones, también llamados servidores proxy, funcionan como un intermediario en cuanto a las peticiones de un cliente a otro servidor y determina cuales de esas peticiones pueden seguir su camino y cuales se cortan. Los cortafuegos de stateful inspection poseen la capacidad de conservar el estado de las sesiones a través de lof firewalls y los híbridos que son una combinación de las características de los tipos mencionados anteriormente.

Otro concepto que es importante retomar cuando hablamos de los cortafuegos son las DMZ (Demilitarized Zone) que constituyen “una red compuesta por uno o más ordenadores que se sitúan lógicamente entre la red corporativa e internet.” (Abad, 2013, pag 167), donde su principal función es dar servicios a internet, pero manteniendo la protección de los datos de la red de la organización.

Diaz, Alzorriz y Sancristobal(2014, 218) mencionan que entre las ventajas que pueden tener los firewalls están que son un punto fuerte en cuanto a las políticas de seguridad, que toleran métodos de autenticación avanzados como los smartcards, su ubicación es beneficiosa para hacer análisis

de tráfico y además necesitan muy pocos usuarios para su mantenimiento. Sin embargo, existen también desventajas en el uso de estas herramientas como el hecho de que pueden limitar el uso de algunos servicios por no ser considerados seguros o que pueden constituir un cuello de botella para el tráfico así como dar a los usuarios una falsa sensación de seguridad.

2.3.4. Tunneling

Vacca (2013) define el tunneling como un método en el cual se colocan paquetes de un protocolo en la carga de otro, esto quiere decir que va a existir un paquete exterior que va a funcionar como medio por el cual se va a transportar un paquete interior. Esta estrategia se suele utilizar para conectar hosts a través de otras redes. Una analogía que utiliza Tanebaum para describir este metodo es:

> Considere una persona que maneja su auto de París a Londres. En Francia, el auto se mueve con su propia energía, pero al llegar al Canal de la Mancha, se carga en un tren de alta velocidad y se transporta a Inglaterra a través del Eurotúnel.(Tanebaum, 2013, 369)

En la analogía anterior podemos interpretar que la conexión interna correspondería al auto de la persona y el eurotúnel sería la conexión interna que en un tramo de recorrido que tiene que hacer se encarga de transportar a la conexión interna.

El ya mencionado IPsec corresponde a un ejemplo de protocolo de tunelización ya que todo el paquete IP se encapsulará en un nuevo paquete IP donde se le añadirá una cabecera, que puede ser AH o ESP, y también otra cabecera IP nueva. Algunos otros ejemplos son el túnel SSL (Secure Sokets Layer, actualmente llamado TLS, Transport Layer Security) que permite lograr conexiones seguras, PPTP (Point to Point Transport Protocol) es "un protocolo que encapsula los paquetes procedentes de las redes de área local de modo que se hacen transparentes a los procedimientos de red utilizados en las redes de transporte de datos" (Abad, 2013, pag 154), el L2TP(Layer Two Tunneling Protocol) que brinda un acceso seguro a redes privadas a través de internet y por último el SSTP(Secure Socket Tunneling Protocol) que brinda un túnel cifrado que emplea SSL/TLS, el cual se suele utilizar para brindar protección a los correos electronicos ya que encripran la información y bloquean el acceso tanto al contenido del correo como a la información de los usuarios involucrados.

La principal ventaja que permite la tunelización es que, ya que encapsula los paquetes, permite que a pesar de que ciertas redes no permitan algunos protocolos aun así se puedan trasladar los paquetes. Sin embargo, Tanenbaum (2003, pag 369) presenta una desventaja, la cual hace referencia a que cuando se utiliza no se logra llegar a los hosts que participan en la red que emplea la tunelización porque los paquetes que son transmitidos no desviarse cuando van por el túnel.

2.4. Redes MPLS

También conocidas como redes de Conmutación Multiprotocolo Mediante Etiquetas. Esta es una nueva tecnología, que tiene como objetivo reducir los posibles problemas que pueden ocurrir durante un reenvío de paquetes en la interconexión desarrollada en la actualidad. Es un estándar de IETF (Grupo de Trabajo de Ingeniería de Internet, del inglés Internet Engineering Task Force)

que a su vez forma parte de RFC 3031. El objetivo principal es lograr que se estandarice una tecnología que integra el paradigma del reenvío de intercambio de etiquetas junto con el enrutamiento desarrollado en la capa de red; se espera que mejore el rendimiento de dicho enrutamiento, que mejore la escalabilidad de la capa de red y que a su vez, brinde más flexibilidad en la entrega de los servicios de enrutamiento (Pepelnjak y Guichard, 2001).

Este protocolo realiza el enrutamiento etiquetando los paquetes, lo cual permite que se agilice el tratamiento que se le da a cada paquete en cada uno de los nodos que están dentro del dominio MPLS. Permite hacer un enrutamiento explícito, el cual se compone por enrutadores de frontera el cual corresponde a LER (Enrutador de Etiquetas de Borde, del inglés Label Edge Routers) y de enrutadores que funcionan para la comunicación de etiquetas, ese es el LSR (Enrutador de Comunicación de Etiquetas, del inglés Label Switched Router), estos también están conformados por un plano de control y un plano de datos; estos enrutadores tienen como función construir las tablas de enrutamiento, el intercambio de etiquetas, señalización de datos y también puede aplicar un enrutamiento flexible que se basa en asignar flujos de extremo a extremo dentro de un dominio autónomo (López, Barón y Puentes, 2007).

Las redes MPLS funcionan de la siguiente manera:

> MPLS agrega una etiqueta en frente de cada paquete; el reenvío se basa en la etiqueta en vez de la dirección de destino. Al convertir la etiqueta en un índice de una tabla interna, sólo es cuestión de buscar en la tabla la línea de salida correcta. Mediante el uso de esta técnica, el reenvío se puede llevar a cabo con mucha rapidez. (Tanenbaum y Wetherall, 2012, p. 403)

Para poder agregar la etiqueta al paquete, se creó un nuevo encabezado de tipo MPLS enfrente del encabezado IP que tiene cada paquete. Este encabezado es genérico y tiene un tamaño de 4 bytes y cuatro campos. El campo con más importancia es el campo denominado Etiqueta, el cual contiene el índice del paquete. Después le sigue el campo de QoS, que corresponde a la clase de servicio. El campo relacionado al apilamiento de múltiples etiquetas es el campo S. El último campo denominado TtL, se encarga de indicar cuántas veces se va a poder enviar el paquete en cuestión. Se va a decrementar en cada enrutador y si este llega a 0, el paquete será descartado (Tanenbaum y Wetherall, 2012). En la siguiente ilustración se pueden identificar mejor dichos campos.

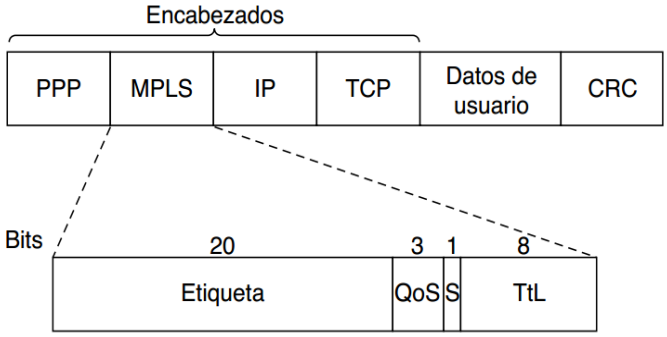

Figura 11: Transmisión de un segmento TCP mediante IP, MPLS y PPP

El MPLS se localiza entre el protocolo IP que pertenece a la capa de red y el protocolo PPP que

forma parte de la capa de enlace. Es dependiente de las direcciones IP o de alguna otra capa de red para poder crear las rutas que van a seguir los paquetes en el proceso, es por esta razón que se dice que no es un protocolo de capa 3 y muchas veces se le llama protocolo de capa 2.5. Los encabezados mencionados anteriormente no forman parte de los paquetes que pertenecen a la capa de red ni de la de datos, MPLS es independiente de estas. En otras palabras, esto significa que se puede construir switches con arquitectura MPLS que cumple la función de reenviar paquetes que sean o no IP; esta es la razón por la cual se le denomina "multiprotocolo" (Tanenbaum y Wetherall, 2012).

El LSR y LER son los nodos principales que forman parte de una red MPLS, participan en los mecanismos del protocolo MPLS. Un LSR es un enrutador de gran velocidad, en una red MPLS se encarga de ser parte de la creación de las LSP (Intercambio de Rutas por Etiqueta, en ingles Label Switching Path) por medio del uso del protocolo de señalización adecuado y ayuda a conmutar de manera acelerada el tráfico de datos presentado entre los caminos que se han establecido previamente. Se le suele llamar enrutador del interior del dominio MPLS. Para poder hacer el uso de las LSP, cada LSR debe tener en sus tablas de envío lo siguiente: la interfaz de entrada y interfaz de salida cada una con su respectiva etiqueta asociada; este es el proceso de distribución de etiquetas. El LER es el enrutador que está en la frontera de una red de acceso hacia una red de tipo MPLS. Cumple dos funciones principales; la primera ocurre en el ingreso, es el encargado de establecer una LSP para el tráfico y después lo envía hacia la red MPLS por medio del uso del protocolo de señalización de etiquetas y la segunda se desarrolla en la salida, acá se encarga de la distribución del tráfico hacia la red de acceso que corresponda; por esta razón es de gran importancia en el proceso de asignar y remover las etiquetas que son aplicadas al tráfico que está entrando y saliendo de una red de tipo MPLS (Llerena y Villacob, 2004).

2.5. Seguridad de Correo Electrónico

Enviar un correo electrónico es como enviar un carta o una postal, cualquier persona que llegue a interceptarla puede leer lo que contiene. Para hacer que el correo electrónico sea confidencial y auténtico, se deben utilizar técnicas criptográficas, para que solo el destinatario pueda ver el contenido del mensaje enviado. Las técnicas más utilizadas para poder brindar este tipo de seguridad al correo electrónico corresponden a PGP y S/MIME.

2.5.1. PGP: Privacidad Bastante Buena

PGP (Privacidad Bastante Buena, del inglés Pretty Good Privacy) es un proyecto creado por Phill Zimmerman en los 90's. PGP proporciona un servicio basado en la confidencialidad y la autenticación que se puede utilizar en aplicaciones que se usan para almacenamiento de datos y para correo electrónico. En este proyecto se seleccionaron los mejores mecanismos criptográficos para usarlos como bloques de construcción, se integraron dichos algoritmos en una aplicación que es de propósito general y que no depende del sistema operativo o del procesador de la máquina, hizo que el paquete y el código fuente estuvieran disponibles (Chapter 12 Pretty Good Privacy (PGP), s.f.).

Este sistema de correo electrónico hace uso tanto de criptografía asimétrica como de la simétrica, esta ultima para poder tener más eficiencia. Su gran ventaja es que ofrece gran facilidad de uso para los usuarios, como por ejemplo para poder crear y gestionar claves (Salazar Almeida, 2007). "Para encriptar los datos, PGP utiliza un sistema de cifrado de bloque llamado IDEA (Algoritmo

Internacional de Encriptación de Datos, del inglés Internacional Data Encryption Algorithm), el cual utiliza claves de 128 bits" (Tanenbaum y Wetherall, 2012, p. 722).

PGP soporta cuatro diferentes longitudes de tipo RSA para que los usuarios creen sus claves, estas son:

1. Casual (384 bits): en la actualidad se puede quebrantar con facilidad.
2. Comercial (512 bits): organizaciones de tres letras pueden quebrantarla.
3. Militar (1024 bits): nadie de este mundo puede quebrantarla.
4. Extraterrestre (2048 bits): ni siquiera alguien de otro planeta puede quebrantarla.

(Tanenbaum y Wetherall, 2012, p. 725)

Proporciona al usuario un "anillo de llaves"o llavero, el cual corresponde a un único fichero donde dicho usuario puede guardar todas sus claves, para que pueda realizar una inserción y extracción de estas mismas de manera más fácil y rápida (Salazar Almeida, 2007).Estos se dividen en dos: anillo de clave privada y anillo de clave pública. En el anillo de clave privada se guardan entre uno o más pares conformados por clave pública/privada que son de carácter personal del usuario, brinda al usuario el beneficio de poder cambiar las claves públicas de forma regular; cada par de estas claves tiene su propio identificador, lo cual hace que el emisor pueda designar al destinatario cual clave pública usó para poder hacer la encriptación. Por su parte, el anillo de clave pública, dentro de este se guardas todas aquellas claves públicas de los contactos del usuario, son necesarias para poder realizar el proceso de encriptación de las claves de mensajes que se asocian a cada mensaje que va a ser enviado por el emisor (Tanenbaum y Wetherall, 2012).

Existen tres requisitos para las claves mencionadas anteriormente:
1. Es necesario un medio para poder generar claves de sesión impredecibles.
2. No hay alguna correspondencia uno a uno entre los usuarios y sus claves públicas. Se necesitan medios para poder identificar algunas claves particulares.
3. Cada entidad PGP tiene que mantener un archivo de sus pares de claves públicas/privadas, como un archivo de claves públicas de corresponsales (Chapter 12 Pretty Good Privacy (PGP), s.f.).

2.5.2. S/MIME

Para comprender dicho sistema primero se debe conocer que es un MIME (Extensiones Multipropósito de Correo, del inglés Multipurpose Internet Mail Extensions). Estas extensiones permiten a los correos electrónicos mensajes que no sean ASCII, mensajes no textuales, cuerpos de mensajes de varias partes y sus encabezados con información que no corresponde a la codificación ASCII. Los mensajes de este formato puede tener archivos de diversos tipos, el tipo de archivo es el que se describe en un encabezado de "tipo de contenido" que es usado por el programa de correo electrónico que utilice el destinatario para poder determinar como usar ese archivo (Al-Janabi y Ibrahem, 2006).

S/MIME (Extensiones Multipropósito de Correo Seguras, del inglés Secure/Multipurpose Internet Mail Extensions) facilita el envío y la recepción de datos MIME de una forma segura. Se encarga de proporcionar servicios encargados de la seguridad criptográfica en aplicaciones que tienen como funcionalidad la mensajería electrónica, algunos de estos servicios son: confidencialidad

de los datos (por medio de la encriptación), autenticación, integridad de los mensajes y no repudio de origen de los mensajes (utilizando firmas digitales) (Al-Janabi y Ibrahem, 2006). Los mensajes usados se componen de cuerpos MIME y de objetos de Sintaxis de Mensajes Criptográficos (CMS, del inglés Cryptographic Message Syntax). S/MIME solo utiliza cuatro tipos de contenido CMS, que corresponden a:

- Datos: el emisor debe usar el identificador de tipo de contenido "id-data" para poder identificar el contenido del mensaje MIME.
- Datos Firmados: usado para aplicar una firma digital a un mensaje o cuando se tiene que transmitir certificados.
- Datos Envueltos: se usa para aplicar la confidencialidad de los datos a un mensaje en específico. El remitente debe tener el acceso a un clave pública para que cada destinatario de dicho mensaje pueda usar este servicio.
- Datos Comprimidos: usado cuando se deben comprimir los datos. Solo se necesita para reducir el tamaño del mensaje (Al-Janabi y Ibrahem, 2006).

Según lo dicho por Tanenbaum y Wetherall (2012):

> S/MIME no tiene una jerarquía de certificados rígida que comienza en una sola raíz, lo cual había sido uno de los problemas políticos que condenaron al fracaso a un sistema anterior conocido como PEM (Correo con Privacidad Mejorada). En su lugar, los usuarios pueden tener varias anclas de confianza. Un certificado se considera válido siempre y cuando se pueda rastrear hacia alguna ancla en la que el usuario confíe.

3. Conclusiones

La seguridad en los diversos tipos de redes es un aspecto de gran importancia que siempre se debe tomar en cuenta, ya que brinda a los usuarios confianza a la hora de utilizar algún programa, aplicación o página web, que implementa algún tipo o técnica de seguridad mencionada y desarrollada a lo largo de este trabajo. A su vez, estas técnicas le brindan el beneficio a los usuarios, para que estos mismos no estén propensos a ataques que podrían ocasionar que extraigan sus datos o información personal o hasta confidencial. Por ejemplo, el uso de la seguridad en las redes permite que entidades como los bancos, que manejan y manipulan información de las cuentas bancarias de empresas, personas u otras entidades, estén menos propensos a los ataques ocasionados por personas que buscan robar este tipo de información.

Con respecto a como interacciona nuestro tema con respecto a los demás temas expuestos por los compañeros de curso podemos ver una gran influencia en lo que son las herramientas para el diagnostico de red en especifico "telnet". Con esta herramienta se pueden crear conexiones conexiones en redes internas y también se usa para la revisión de los diferentes puertos para comprobar su estado, para esta comparación nos enfocaremos solo en el primero de sus usos mencionados.

Con "telnet" la información viaja de una terminal a otra sin ningún tipo de cifrado, solo se envía el texto plano. Es evidente por que esto es un gran problema si se usara en redes que no fueran de confianza. Es por esto que se usa un protocolo llamado "SSH"(Secure Shell), que es donde el tema se relaciona con el expuesto en nuestro trabajo ya que para implementar dicho tipo

de protocolo y poder evitar las vulnerabilidades de “telnet” se usa un cifrado como el RSA para encriptar el texto plano convirtiéndolo en un mensaje altamente cifrado.

4. Bibliografía

- Abad Domingo, A. (2013). Redes locales. McGraw-Hill España. https://elibro-net.ezproxy.sibdi.ucr.ac.cr/es/ereader/sibdi/50228?page=155
- Al-Janabi, S., y Ibrahem, M. T. (2006). Secure E-Mail System Using S/MIME and IB-PKC. In Proceeding of the 6th International Philadelphia Engineering Conference (IPEC 2006), Amman, Jordan (pp. 19-21). Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3467481
- Chapter 12 Pretty Good Privacy (PGP). (s.f.). Recuperado de: http://www.facweb.iitkgp.ac.in/šourav/PGP.pdf
- Cosoi P., Eduardo. (2005). Redes Privadas Virtuales: Un mundo de acceso a las librerías del mundo. Revista chilena de pediatría, 76(2), 207-208. https://dx.doi.org/10.4067/S0370-41062005000200014
- Díaz Orueta, G. Alzórriz Armendáriz, I. y Sancristóbal Ruiz, E. (2014). Procesos y herramientas para la seguridad de redes. UNED - Universidad Nacional de Educación a Distancia. https://elibro-net.ezproxy.sibdi.ucr.ac.cr/es/ereader/sibdi/48736?page=489
- González Rodríguez, M. González Rodríguez, M. (Ed.) y Stallings, W. (2004). Fundamentos de seguridad en redes: aplicaciones y estándares (2a. ed.). Pearson Educación. https://elibro-net.ezproxy.sibdi.ucr.ac.cr/es/ereader/sibdi/45309?page=199
- León, D. (2019, 7 junio). ¿Qué otros usos tiene la criptografía aparte de las criptomonedas? CRIPTO TENDENCIA. https://criptotendencia.com/2019/06/06/que-otros-usos- tiene-la-criptografia-a-parte-de-las-criptomonedas/
- Llerena, C. A., Villacob Pineda, K. (2004). MPLS: conmutación de etiquetas multiprotocolo. (tesis de pregrado). Universidad Tecnológica de Bolívar, Colombia.
- López, D. A., Barón, J., Puente, F. J. (2007). Optimizando la transmisión de datos IP mediante la conmutación de etiquetas multiprotocolo. Ingeniería, 12(2), 62-67.
- Kurose, J. F. y W. Ross, K. (2010). Redes de computadoras: un enfoque descendente (5a. ed.). Pearson Educación. https://elibro-net.ezproxy.sibdi.ucr.ac.cr/es/ereader/sibdi/52539?
- Rabenstein, M. (2020, 22 julio). ¿Qué hace una empresa de alojamiento web para tu sitio web? noticias.ltda. https://www.noticias.ltda/seguridad-informatica/cifrado-de-correo-electronico/
- Pepelnjak, I., Guichard, J. (2001). MPLS and VPN Architectures. Recuperado de: https://doc.lagout.org/network/Cisco/Cisco %20Press %20Collection/Cisco %20Press %202001 %20- %20 MPLS %20and %20VPN %20architectures.pdf

- Salazar Almeida, B. G. (2007). Esquemas de Seguridad de Correo Electrónico.(tesis de grado). Escuela Superior Politécnica del Litoral, Ecuador. Recuperado de: https://www.dspace.espol.edu.ec/bitstream/123456789/10538/3/ESCUELA %20SUPERIOR %20POLIT %c3 %89CNICA %20 DEL %20LITORAL.pdf
- Tanenbaum, A. S. (2003). Redes de computadoras (4a. ed.). Pearson Educación. https://elibronet.ezproxy.sibdi.ucr.ac.cr/es/ereader/sibdi/107745?page=1
- Tanenbaum, A., Wetherall, D., y Romero Elizondo, A. (2012). Redes de computadoras. Mexico: Pearson Educacion.
- Vacca, J. R. (2013). Computer and information security handbook. ProQuest Ebook Central https://ebookcentral-proquest-com.ezproxy.sibdi.ucr.ac.cr
- Venturini, G. (2020, 24 junio). ¿Qué es la Criptografía? Tecnología + Informática.https://www.tecnologia-informatica.com/que-es-la-criptografia/
- Wu, P. (2019, 27 noviembre). Explicación del cifrado de DNS. The Cloudflare Blog.https://blog.cloudflare.com/es/dns-encryption-explained-es/