UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

ENEP ARAGÓN

PRINCIPIOS DE E-COMMERCE CON SEGURIDAD INTEGRADA.

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

JORGE CRUZ VÁZQUEZ

ASESOR: ING. Alejandro R. González Ponce

MÉXICO, DF. SEPTIEMBRE 2003

AGRADECIMIENTOS.

A mi papá Dr. Angel Cruz Espinoza.

Gracias por darme la libertad de buscar mis anhelos siempre dándome el apoyo y la confianza de cada paso que tomaba, gracias por enseñarme tantas cosas de la vida.

A mi mamá Mtra. Gloria Vázquez Gómez.

Gracias mamá por tanto cariño y amor que a diario me das el cual me impulsa día con día para conseguir mis sueños.

A mi hermano Dr. Angel Cruz Vázquez.

Por darme el ejemplo del estudio, de saber que las cosas que uno anhela siempre se pueden lograr.

A mi hermana Dra. Vianney Cruz Vázquez.

Por darme tú apoyo y ayuda en todo momento, gracias por tú cariño.

A mi hermana Dra. Magaly Cruz Vázquez.

Por darme una sonrisa cuando la necesite y cariño.

A mi novia Dra. Claudia Torres Romero

Por tú amor, atención, tiempo y sobre todo comprender mis sueños que quiero conseguir.

Índice general

Introducción

El fenómeno socio-cultural y comercial que ha traido consigo el Internet tiene como origen la década de los 60's y es relacionado con el proyecto de defensade los Estados Unidos. En la década de los 90's con el gran apogeo de Internet, donde Internet es parte de una gran herramienta de comunicación, difusión e integración de la información.

Con la introducción de las nuevas tecnologías de la información se está construyendo una revolución cuya importancia esta siendo comparada con la que tuvo la revolución industrial a fines del siglo XVIII.

En menos de una década habrá cambiado la forma de interrelación entre las empresas, la estructura y organización de los mercados, y la forma en que las personas se educan , trabajan , consumen , ahorran y se entienden asociadas al proceso de informatización de la sociedad.

El efecto económico que traera consigo un impacto directo sobre los productores, distribuidores y consumidores modificando el ritmo de productividad y el crecimiento de los países.

La revolución de la tecnología de la información traerá consigo un cambio permanente en la estructura productiva y en la cadena de distribución de los bienes y servicios así como la gestión de las empresas.

Una esperanza de que este tipo de economía pueda cerrar la brecha entre las grandes potencias y la competencia entre países, es cada vez mayor debido a que se trata de una inovación tecnológica, los primeros en implementarlas son las economías avanzadas pagando el precio los países menos desarrollados.

Comunicación e integración que le permiten a los usuarios ahorrar tiempo y dinero, además de tener a su alcance los productos y servicios que requieren, sin fronteras de espacio y tiempo.

A medida del crecimiento exponencial del uso del web, así como el desarrollo de comercio electrónico, es importante la seguridad de la información que transita a través del medio. El canal de comunicación que se utiliza en Internet es bidireccional pero cabe mencionar que dicho canal presenta una vulnerabilidad, debido a que es realmente inseguro por parte de su naturaleza en como fue creado.

El transito de información que se da a diario por el web es en demasia inseguro, toda o la mayoría de la información que por el viaja lo hace de manera transparente, de forma que nosotros escribimos nuestros mensajes los cuales son enviados y cualquiera en la red podrá verlos.

Para poder lograr esto existen herramientas gratuitas en internet que una tercera persona podría utilizarla para obtener información agena y violar la privacidad de los usuarios. Quizás esto no tenga mucha importancia si solo se envía un correo electrónico notificando una noticia a un amigo, pero imagine si se esta realizando una transacción económica o si deposita la confianza en un servicio Web comprando un producto y dando su número de tarjeta de credito.

La prima más importante es la información y hoy en día ha cobrado un peso muy importante y se ha llegado a decir que la información da poder. En el caso de las empresas de gran peso y renombre, la competencia de sus productos y del mercado virtual es importante, tanto la proyección que puedan lograr por el web como la confiabilidad que puedan proyectar a sus clientes.

De aquí la gran importancia que ha cobrado en los últimos años la utilización de métodos de seguridad en web y el poder proporcionar servicios seguros de web, tanto a nivel del usuario como a nivel comercial.

El conocer ampliamente el mercado de trabajo en que se enfocan cada uno de los esquemas que existen del e-commerce nos facilitará las cosas para entender y saber a que tipo de mercado queremos llegar y cúal es la arquitectura que debemos adoptar para su implementación.

Empaparnos de los conocimientos básicos con que se rige la seguridad informática nos permitirá de una manera más clara entender los mecanismos de seguridad que debemos adoptar dependiendo nuestras necesidades aplicandolo en su caso a nuestro sitio e-commerce.

Además sabremos cómo instalar un servicio seguro por medio de códigos fuentes libres disponibles en la red así también del apoyo de software libre para la implementación de nuestro sistema y por último cabe señalar que es de suma importancia saber como funciona internamente nuestra herramienta de seguridad que utilizaremos por lo cual se explicará a detalle SSL.

Capítulo 1

Fundamentos de e-commerce

1.1. Qué es el e-commerce

Entender el término de e-commerce se nos puede venir a la mente varias cosas que quizas no describan totalmente la definición formal de e-commerce. Podriamos imaginarnos que podrían ser alguna de las siguientes ideas :

- Una pagina Web
- Un catálago de Productos
- Un montaje de negocio sobre Internet
- Un método de pago

Antes de comenzar con definiciones formales cabe mencionar de donde forma parte importante el comercio electrónico y su conformación.

E-business.

Se entiende el termino de e-business o negocio electrónico al conjunto de aspectos relacionados con la gestión de negocios de las empresas que utilizan la Tecnología de la Información[1], a través de internet para mejora de sus áreas, donde el aspecto más visible del e-business es el comercio electrónico.

En términos generales el comercio electrónico es la posibilidad de realizar transacciones comercionales a través de un medio electrónico, donde interacciona un cliente el cual requiere un producto o servicio y un proveedor que lo proporciona, este último publica sus ofertas y si al cliente le satisfacen sus necesidades se raliza la venta.

[1] También conocida por la abreviación TI

1.1.1. Definiciones

A continuación se darán distintas deficiones que describen el comercio electrónico:

1. Toda forma de transacción o intercambio de información comercial basada en la transmisión de datos por red de telecomunicaciones como Internet.[12]
2. Práctica de vender y comprar productos y servicios alrededor de internet, con la ayuda de nuevas tecnologías entre las que se destaca la web, intercambio de datos electrónicos, e-mail, transferencias electrónicas, tarjetas electrónicas.[7]
3. El uso de la red con fines de realizar comercio y otras actividades económicas, donde los bienes y servicios son producidos, diseñados, comprados, inventariados, enviados y contabilizados, donde se involucran empresas privadas, pequeñas y medianos empresarios así también organizaciones gubernamentales y educativas.[1]

En base a las definiciones anteriores podemos decir que el término de **e-commerce** es aquel que describe conceptos interrelacionados y fenómenos de negocio, como los son comprar un libro, verificando el estado de cuenta del banco, todo esto con ayuda del Web.

Esta actividad comparte 2 generalidades importantes :

1. Todas son relacionadas a actividades de negocio y comercio.
2. Los sistemas corren sobre la plataforma de internet y utilizan el word wide wibe.

El entorno de trabajo del **e-commerce** lo describe como el conducto de las actividades de negocio, haciendo uso de la plataforma de Internet y el protocolo http[2]

El uso libre de las llamadas telefónicas para realizar un pedido no envuelve al **e-commerce** , mientras que esta es una actividad relacionada al negocio, no hace uso del internet. Las actividades de reventa, tales como la compra desde casa, que utilizan medios como la televisión o la telefonía no constituyen un e-commerce, basandonos en la definición.

Esta definición restrictiva nos ayuda a enfocarnos sobre los negocios que se encuentran enfocados dentro de la plataforma de Internet y la Web.

[2]hipertext transfer protocol

Estas definiciones de **e-commerce** no incluyen el intercambio electrónico de datos (EDI[3]), que es la tecnología que algunas industrias utilizan para permitir que sus computadoras intercambien datos. Mientras que estas actividades relacionadas al negocio y están siendo dirigidas sobre la plataforma de las telecomunicaciones las cuales no hacen uso de Internet.

Posteriormente abarcaremos la iniciativa de EDI de los 80's la cual se extendió para conformar el e-commerce.

1.1.2. Ventajas

Bueno pero Qué ventajas nos proporcionaría el implementar el comercio electrónico ?.

Algunas de la ventajas útiles que trairía consigo serían las siguientes:

- No necesitamos de un local físico para poder proporcionarle una atención al cliente.
- No requerimos de personal para la atención a nuestros clientes.
- No pagaríamos horas extras, y se podrá dar un servicio de 24 hrs los 365 días del año.
- Es accesible desde cualquier rincón del mundo.

Una vez dado algunas definiciones y las bondades que nos proporcina debemos de tener en claro que podemos distinguir distintas clases de comercio electrónico que varían en función de tres factores importantes :

1. Según la relación cliente - proveedor.
2. Según el proceso de compra.
3. Según el medio utilizado.

1.2. Clasificación según su relación.

En el año de 1991 no estaba permitido realizar transacciones comerciales a través del Internet, establecido en las políticas de uso aceptable de la Fundación Cientifica Nacional[4] de los Estados Unidos encargada de estos rubros y prohibía explicitamente toda transacción comercial por medio del Internet. En ese mismo año se creo la Asociación de Intercambio comercial sobre Internet[5], una organización que se dedicó a estudiar y promover los posibles usos comerciales.

Las primeras transacciones comerciales en internet surgieron en los años de 1993 y 1994 , en Estados Unidos.

[3]electronic data interchange
[4]National Sciencie Foundation
[5]CIX Association - Commercial Internet Exchange

Ya en este entonces ya era posible la adquisición de software y servicios informaticos a través de la red, aunque la compra de productos parece timida desde el punto de vista del consumidor. En poco más de dos años , las transacciones habían aumentado de 8 millones en el años de 1994 a 2 ,900 millones en el años de 1996.

Podemos destacar entre los siguientes tipos de comercio electrónico :

1. Business to Business (B2B)
2. Business to Consumer (B2C)
3. Business to Goverment (B2G)

Cada uno de los tipos de comercio electrónico que se mecionan pueden estar enfocados con un fin distinto, presentando ventajas y desventajas cada uno es sus ramas de aplicación.

1.2.1. Business to Consumer

B2C es el comercio electrónico que se da entre un **negocio** y **el consumidor final**, donde el consumidor final es tambieén conocido como el consumidor directo.

En este tipo de módelo de comercio electrónico se enfoca a todos aquellos que venden sus productos a través de internet y que son diriguidos al público en general. Además permite al consumidor realizar sus compras más comodamente y le brinda a las empresas realizar el seguimiento de las mismas, dar soporte al comprador y la posibilidad de afianzar las relaciones con sus clientes habituales y nuevos.

Cabe mencionar que el cliente final utiliza directamente la plataforma de Internet, particularmente la Web, para realizar actividades como buscar, ordenar y realizar pagos. El Internet no es la primera plataforma que ha proveido al cliente la posibilidad de realizar compras desde el hogar haciendo uso del medio de telecomunicaciones, aunque más de estos esfuerzos no tuvieron éxito.

Historia de B2C

Desde los principios de los 80's, los negocios han estado tratando de proveer a los clientes finales a través de una alternativa electrónica visitar su negocio virtual. Todo esto comenzó con servicios de información que podían ser accesados desde su hogar.

Uno de los primeros esfuerzos fue realizado por la compañia Boston's Citinet la cual ofreció una variedad de servicios como el e-mail electrónico, catalogos de bienes y oportunidades de empleo. Otro popular servicio que brindo la compañia de Prodigy fue la reservación de vuelos en aerolíneas y la compra desde casa.

En el año de 1984 otro esfuerzo fue forjado por la empresa Chase Manhattan la cual inaguro un sistema de banco en casa, en colaboración con AT&T. El cliente podía realizar una conexión al banco y poder desplegar su estado de cuenta sobre su televisión haciendo uso de un dispositivo que debía ser proveido por AT&T. En esta epoca las computadoras personales no eran muy populares por lo que AT&T tuvo que hechar mano en el desarrollo de un dispositivo de reensamblado que estaba compuesto por un teclado y una tarjeta lectora.

El cliente podía insertar su tarjeta y con el teclado podía realizar una conexión telefónica al banco, mientras que la televisón podría desplegar la información de su estado de cuenta y así también poder efectuar transacciones con ayuda del teclado proporcionado. El cliente en un principio reacciono entusiastamente en las pruebas de la tecnología.

Pero tal aventura tuvo un gran fracaso debido a lo voluminoso de los cables sobre el piso que la instalación requería colocar en el cuarto donde se efectuaría la conexión y por ende donde se encontraba el televisor, el teléfono, por tales cambios en su casa no tuvo éxito tal proyecto.[1]

Actividades en B2C

La interacción entre el negocio y el cliente final consiste de las siguientes actividades :

- Promoción.
- Orden.
- Entrega del Producto.
- Después de la venta el Soporte.

En cada una de estas áreas, la plataforma de e-commerce juega un roll importante. Avisos en el sitio del portal son desplegados de igual manera de como se realiza en la TV, el periódico o se escuchan en la radio.

Libros, vestidos, mobiliario y cd's pueden ser ordenados a través del Internet, un producto digital tal como la música o el software pueden ser descargados y posteriormente después de la venta los servicios se pueden llevar a cabo por e-mail o el sistema de preguntas más frecuentes.

Cabe señalar que el mayor desembolso de publicidad que se realiza se da en Internet, teniendo un ingreso en el año de 1999 de $ 3.3 billones de dolares y se espera que para el año 2004 sea de $ 33 billones de dolares donde el 8 % de toda la publicidad se realizará sobre Internet, este tipo de publicidad hace uso de banners, botones y abundantes slogans animados.[7]

Algunas de sus ventajas y desventajas se describen a continuación.

Ventajas

- Puede encontrar una gran ventaja por no existir un intermediario entre la relación entre el vendedor y el consumidor, habiendo un ofrecimiento directo del producto al consumidor.
- Tanto grandes como pequeñas empresas pueden proyectar sus productos sin tener que realizar fuertes inversiones.
- No es necesario grandes cantidad de inventario físico , si no grandes estrategias de distibución.
- Ayuda a mejorar la imágen de una empresa.

Desventajas

- Alta demanda de competencia entre las empresas que manejan el mismo módelo.
- Falta de infraestructura de telecomunicaciones.
- Altos costos por el uso telefónico.
- El servicio que se proporcione marcara la diferencia.
- Existen muy pocos márgenes de utilidad.
- Falta de difusión de tarjetas de crédito.

Tipos de B2C.

Una vez dado un panorama general del B2C y mostrado sus pros y contras cabe mencionar que entre los tipos de B2C que se encuentran dependiendo del servicio que ofrecen al consumidor se encuentran los siguientes:

- Portales Generalistas Horizontales.- Pretenden satisfacer todas las necesidades del consumidor.
- Portales Especializados Verticales.- Se enfocan únicamente a una área en especifica y contienen toda la información y servicios de la misma.
- Comunidad Virtual.- Se centran en brindar servicios de comunicación como lo son los foros de debate, chat's , alojamiento de web's , etc.

- Tiendas Virtuales.- Toda tienda que vende a través de internet, las cuales pueden ser :
  - Fabricantes con el fin de eliminar intermediarios,
  - Tiendas que ya existen fisicamente y encuentran un canal más de expanción.
  - Tiendas creadas exclusivamente para el mundo de internet.
- Centros Comerciales Virtuales.- Agrupan muchas tiendas virtuales y le permiten al consumidor pasar de una a otra con facilidad.
- Subastas.- Los productos son realizados entre consumidores.

1.2.2. Business to Business

B2B comercio electrónico que se raliza entre negocios.

Este tipo de comercio no es nuevo en la actualidad, por lo general las empresas simpre realizan compras para suministrar sus operaciones. Lo que se modifica son sus formas de operar y sus estructuras de costo,desaparecerán los grandes departamentos de compras y se reducirán al máximo los trámites burocráticos.

Sus requerimientos de abastecimiento y especificaciones los realizarán ahora a través de portales B2B y a través del medio recibirán múltiples ofertas de parte de los proveedores. Este tipo de módelo se encuentra enfocado a otro tipo de personas, es decir, a distribuidores y proveedores, este tipo de comercio electrónico se encuentra mucho más restringido.

Podemos mencionar que en B2B se descarga la mayor cantidad de recursos económicos y debe existir una relación estrecha entre el distribuidor y proveedor.

En cuanto al funcionamiento de las empresas este mecanismo podrá optimizar las funciones de abastecimiento y distribución de sus productos.

VENTAJAS

- El proveedor puede mostrar sus inventarios a los distribuidores
- Permite la revisión de estados de cuentas y pagos de los mismo.

DESVENTAJAS

- No toman mucho en cuenta al consumidor final.

Desde el punto de vista de la inversión que pueda originar una red de transacciones B2B en un futuro próximo es muy difícil realizar un estimado, debido a que cada empresa presenta diferentes exigencias y necesidades , por lo que que se prevee todo un rumbo hacia las Redes Privadas de Intercambio lo cual fortalecerá la información y la cooperación entre los distribuidores y proveedores.

1.2.3. Business to Goverment

En el módelo de B2G se establece una relación cooperativa entre las empresas y el gobierno con el fin de optimizar trámites burocráticos.

Un ejemplo práctico es el que se da en E.U. donde el gobierno realiza sus disposiciones a través de internet y las compañías pueden responder electrónicamente, por lo cual está representando un canal potente de presentación de servicios para ciudadanos y empresas.

VENTAJAS

- Permite al gobierno adquirir bienes o servicios a un precio más bajos sin el desgaste de grandes aparatos burocráticos.
- Ahorro de tiempo y dinero en la adquisición de bienes y servicios.
- Reducción de tiempo para solicitar pedidos.
- Herramientas del control del gasto público.

Lo que realmente aporta B2G es la versatilidad en el manejo de la Administración pública y por consecuencia habilita la disponibilidad de los recursos para dirigirlos directamente al ciudadano o en la reducción del endeudamiento. El panorama del B2G no está tan claro ya que lo valioso de este tipo de modelo radica en su posición en comparación con los otros modelos así como la independencia y confidencialidad, lo cual conlleva que aquellas iniciativas independientes puedan tornarse en un futuro en posiciones importantes.

1.2.4. Consumer to Consumer

1.3. Clasificación según el proceso de compra.

El comercio electrónico implica la conjunción del mundo físico a un mundo virtual el cual da origen al proceso de compra. Podemos distinguir entre dos tipos de procesos de comercio electrónico.

PROCESO INCOMPLETO.

En el proceso incompleto todo el proceso entendiendose como proceso a la selección del producto, pago y entrega, se realiza totalmente en línea; esto es únicamente posible con mecarcias que con su naturaleza pueden ser transmitidas por internet (información , datos, cursos).

PROCESO PURO O COMPLETO.

En este tipo de proceso se sigue realizando la selección del producto y pago por medio electrónico, pero en la fase de distribución y entrega debe de realizarce físicamente porque así lo requiere la mercancia (ropa, libros).

1.4. Clasificación según el medio.

Podemos realizar una clasificación por medio del cual se realice el comercio electrónico encontrando las siguientes alternativas de difusión de medios.

1.4.1. Comercio Electrónico por medio de EDI(Electronic Data Interchange).

El EDI asocia las mejores prácticas comerciales con el apoyo de la tecnología, mejorando la relación comercial entre las empresas y sus distintos interlocutores (clientes, entidades financieras, proveedores, administración pública, etc). Convirtiendo además documentos comerciales elaborados en papel en mensajes electrónicos, transmitidos y procesados automáticamente por las aplicaciones sin intervención manual alguna.

1.4.2. Comercio Electrónico por medio de Internet.

Debido al gran exito que ha representado este medio en la última decada y su amplio uso representa una de las grandes ventajas del uso de este medio para poder llegar al consumidor.

La presente tesis utilizará este medio de aplicación para su aplicación.

1.4.3. Comercio Electrónico a través de Televisión Digital.

La televisión digital que permite acceder a Internet sin equipo informático constituye la respuesta ideal para aquellas personas que desean disfrutar de la web, pero que se resisten a comprar una computadora exclusivamente para navegar por Internet.

Podríamos pensar que sería un poco complejo la computadora y su precio bastante elevado para utilizarla únicamente para acceder a Internet. Hasta hace muy poco tiempo no existia ningun otra alternativa para realizar operaciones tan sencillas como navegar, enviar correos o charlar.

La televisión interactiva brinda una combinación de programación de TV e información integrada para una mayor facilidad de uso, además ofrece una solución eficaz debido a que resulta sencillo su manejo como se venía realizando para ver la TV.

La televisión digital brinda una TV normal o un navegador web, para visitar páginas, enviar y leer correos o tener una conversación con los amigos mientras se sigue viendo la TV en un pequeño recuadro en una esquina de la pantalla.

Además que se le pueden conectar perifericos adicionales, como una impresora para poder imprimir las páginas visitadas. El único inconveniente es la resolución de los receptores de TV, muy inferior a la de los actuales monitores de computadoras, lo cual podría dificultar la lectura de ciertas páginas y degradar sus imágenes y efectos gráficos.

1.4.4. Comercio Electrónico por telefonía móvil.

El wap[6] es un protocolo de instalaciones inalámbricas, es decir, es un estándar para la prestación de servicios de información y telefonía sin la necesidad del cable. El objetivo inicial de esté tipo de tecnología es el de proporcionar interoperatividad entre las distintas familias de productos inalámbricos.

El wap llega a través de la telefonía móvil y por medio de él se puede uno conectarse a Internet para poder realizar distintas tareas como por ejemplo transacciones bancarias, comprar , vender, recibir noticias, como el slogan tener Internet en la palma de la mano que mucho utilizan los medios de propaganda.

1.4.5. Comercio Electrónico a través de telefonía fija.

Actualmente muchas páginas web ofrecen un servicio telefónico de apoyo. Muchas empresas consideran el realizar publicidad a través del Internet y el generar un decisión de compra gracias a la información encontrada en una página web es hacer comercio electrónico. Este comportamiento trae consigo que en algunas ocasiones, una venta cuyo inicio se comenzo a través de la red se cierre telefónicamente.

Gran cantidad de empresas operan a trevés de Internet y realizan el cierre de la operación de la compra telefónicamente, donde algunas de estas ventas pueden ser consideradas on-line y otras no.

1.5. Limitaciones de la Web

A pesar de este tipo de metodologías emergentes, el Web como una herramienta de publicidad sufre de algunas desventajas.

[6]Wireless Aplication Protocol

1. Únicamente pequeños banner pueden ser desplegados, todo esto comparado al impacto posible que se puede lograr con la televisión o por páginas completas en periódicos.

2. El navegador se puede considerar que esta fuera de control al poder realizar algun click fuera del sitio web.

3. El costo de los valore utilizados para la publicidad para poder evaluar la efectividad del medio no esta bien establecida para el web.

1.6. Ventajas de la Web

La web visto como un canal de promoción, presenta algunas ventajas sobre los medios pasivos como lo son la televisión y la radio.

1. El web es interactivo y con esto tiene a la persona más envuelta con el medio. El navegar por la web el usuario tiene un mayor control en el sitio que desea visitar y la forma de interactuar con el medio, en comparación con otros medios interactivos que son demasiados limitados y de poca libertad para el usuario, por tal motivo se dice que la web es de una manera más natural.

2. Es mucho más enfocado que la televisión o los periódicos, es decir, la experiencia de la web puede ser ajustada a cada usuario. Esta puede ser convertida como una herramienta de micromercado en conjunto con un diseño de publicidad para cada consumidor, esto con el fin de envolver al usuario llevando el control de la información personal así como los detalles de compras que realice.

3. Es una herramienta participativa, el poder de comunicarse con más personas en línea, por ejemplo los productores con bajo contenido de información pueden promover tales comunicaciones enfocado con un objetivo social o compañias farmaceuticas podrían ayudar a establecer un cancer de corazón.

El desafio de la publicidad basado en la web consiste en aplicar efectivamente el enfoque de interactividad y participación.

1.7. Conclusiones

Conocimos los distintos tipos de e-commerce que existen en la actualidad y el enfoque personal que tiene cada uno de ellos, distinguiendolos unos de otros por el mercado hacia donde se encuentran dirigidos.

Una vez conocida la manera de como trabajan cada uno de ellos podríamos partir con la iniciativa de implementar alguno de estos esquemas dependiendo de las necesidas que tengamos, pero hay que ponder mucho incapie en la parte de seguridad que debe presentar cualquier esquema de e-commerce que vayamos a implementar y los mécanismos que debemos considerar para que nuestro sitio e-commerce cubra con la seguridad mínima que demande un sitio de esta embergadura.

Con tales fines debemos tener un conocimiento básico de que es la seguridad y los mécanismos de seguridad que deben ser implementados en nuestro sitio e-commerce.

Capítulo 2

Seguridad e Internet

2.1. Historia de la Criptografía

La ciptografría es tan antigua como la escritura y se dice que las primeras civilizaciones que usaron la criptografía fueron la Egipcia, la Mesopotamia, la India y la China.

Los espartanos 4000 años antes de Cristo, utilizaban papiro en forma de escritura, el cual consistía en un cilindro al cual se colocaba un papiro en forma de espiral. Se escribía entonces el texto en cada una de las vueltas del papiro, pero de arriba hacia abajo, una vez desenrrollado, sólo se podía leer una serie de letras aparentemente inconexas. Para descrifrar el mensaje era necesario colocar el papiro exactamente en la misma posición en la que había sido escrito.

Antiguos textos judíos fueron cifrados siguiendo el método de sustituir la primera letra del alfabeto por la última y así sucesivamente. En la Biblia el nombre de Babilonia aparece cifrado como "Sheshech".

Pero a quien se la atribuye el primer método de cifrado es al general romano Julio César, quien creó un sistema simple de sustitución de letras, que consistía en escribir el documento cifrado con la tercera letra que le siguiera a la que realmente correspondía, la A era sustituída por la D, la B por la E y así sucesivamente.

Estos sistema tan simples evolucionaron posteriormente a elegir una reordenación cualquiera(permutación) del alfabeto, de forma que a cada letra se le hace corresponder otra ya sin ningún patrón determinado.

Durante la Primer Guerra Mundial se utilizaron extensivamente las técnicas criptográficas, lo que impulsó al final de la guerra, el desarrollo de las primeras tecnologías electromecánicas, un ejemplo claro de ello fue el desarrollo de la máquina Enigma utilizada por los alemanes para cifrar y decifrar sus mensajes.

Con el desarrollo de la informática en la segunda mitad del siglo pasado y con el uso cada vez más extendido de las redes informáticas y del almacenamiento masivo de información se ha dado paso a un gran salto en el estudio de sistemas criptográficos. En 1975 **Diffie y Hellman** son el parte aguas de las bases teóricas de los algoritmos de llave pública, hasta entonces no se concebía un sistema de cifrado que no fuese de clave secreta, en la actualidad se usan distintos métodos criptográficos como DES, RSA, MD5, etc.[12]

2.2. Conceptos Básicos

Supongamos que existe la necesidad de enviar un mensaje a X persona y nosotros quisieramos estar seguros de que nadie más pueda leer el mensaje. Con tal motivo surge la necesidad de proteger nuestra información que enviemos, a través de métodos criptográficos.

El mensaje que nosotros deseemos enviar a través del canal público de Internet será conocido como **Texto En Claro** y el proceso que realiza la distinción del mensaje en su ocultamiento lo conoceremos como **Cifrado**, obteniendo como resultado lo que conoceremos como **Texto Crifado**; el diagrama siguiente esquematizará lo mencionado anteriormente.

2.2.1. Criptología

La **Criptología** es el estudio de la criptografía y el criptoanálisis.[8]

2.2.2. Criptoanálisis

El **Criptoanálisis** es el estudio de las técnicas matemáticas con el fin de derrotar las técnicas criptográficas y más generalmente servicios seguros de información.[8]

2.2.3. Criptoanalista

El **Criptoanalista** es alguien que emplea el criptoanálisis.[8]

2.2.4. Criptosistema

El **Criptosistema** es en términos más generales se refiere a un conjunto de primitivas criptográficas utilizadas para proveer servicios seguros de información , más frecuentemente el término es utilizado en conjunción con primitivas que poseen confidencialidad, es decir, cifrados.[8]

2.2.5. Criptografía

La **Criptografía** es el estudio de las técnicas matemáticas relacionadas con aspectos de la seguridad de la información tales como la confidencialización, integridad , autenticación y no repudio.[8]

2.2.6. Objetivos de la Criptografía

Los objetivos principales que pretende alcanzar la criptografía son los siguientes :

- **Autenticación** Cuando nosotros recibimos un mensaje de cierta persona debemos de estar completamente seguros de que dicha parsona es quien dice ser, es decir que no exista un intruso que false su identidad.
  A esto daremos el término de ***autenticación*** verificar que la persona es realmente es quien dice ser.[9]

- **Integridad** Sabemos de la inseguridad que corre nuestra información a través del canal público de la red, por lo que es necesario el asegurarse que la información que nosotros enviemos o recibamos no haya sido modificada durante su translado, podría darse la situación que un intruso pudiera sustituir nuestra información por una falsa.
  Entenderemos entonces el término de ***integridad*** ; la información que no haya sido mani-pulada sufriendo alteraciones como inserciones , borrado o sustitución.[9]

- **No Repudio** Cuando nosotros recibimos algun mensaje podemos asegurarnos de la autenticidad de la persona pero no cubre la posibilidad de que dicha persona pueda negarse de que él nunca envio el mensaje.

  Supongamos que surgen una disputa entre las dos partes (emisor-receptor) debido a que una entidad niega de ciertas acciones que fueron tomadas por ella, por ejemplo una entidad le concede o le autoriza a otra entidad el poder realizar la compra de algunas propiedades y posteriormente negar tal conceción que se dio; claramente vemos que existe un gran problema de tener un mecanismo que nos garantice las acciones y obligaciones que presenta un servicio y no traten de negar que ellos lo dieron o lo realizan.

  Entenderemos entonces el término de ***no repudio*** como la forma de asegurarnos que dicha persona fue realmente quien realiza una acción y no trate de refutar dicha acción.[9]

- **Confidencialización.** Es el servicio utilizado para mostrar el contenido de información aquellas personas que tengan autorización de verla. Podemos nombrarlo también como secreto un sinonimo de confidencialidad y privacidad , estas son numerosas aproximaciones para proporcionar confidencialidad a través de los algoritmos matemáticos que hacen que nuestra información viaje crifrada (no legible) por el canal.[9]

2.3. Notaciones

Antes de continuar es conveniente definir algunas notaciones que son utilizadas para la comprensión de algunos términos que utilizaremos con frecuencia para denotar los siguientes conceptos: cifrado, decifrado, el espacio de llaves por mencionar algunos.

Cifrado

- Denotaremos con la letra A al conjunto finito del alfabeto de definición, por ejemplo $A = \{ 0 , 1 \}$ representa un alfabeto binario.[8]
- Denotaremos con la letra M al conjunto que representa el espacio de los mensajes. M consiste de las cadenas de símbolos del alfabeto. Debe de quedar claro que un elemento de M será llamado texto en claro o mensaje en claro. Por ejemplo M puede estar formado por cadenas binarias, el texto en algún idioma.[8]
- Denotaremos con la letra C al conjunto que representa el espacio de texto cifrado. Sabemos que C consiste de cadenas de símbolos de un alfabeto, el cual puede diferir del alfabeto por definición de M. Cabe señalar y quedar en claro que un elemento de C es llamado el texto cifrado.[8]
- Denotaremos con la letra K al conjunto que representa el espacio de llaves. Debe de quedar en claro que un elemento de K es llamado llave.[8]

2.3.1. Cifrado y Decifrado

CIFRADO

Definición.- Es el proceso de transformación que sufre el texto en claro en un texto cifrado por medio de un algoritmo matemático y con la utilización de una llave.[11]

Más formalmente podemos decir que cada elemento de $k_1 \in K$ determina únicamente una biyección de M a C, denotado por E_k lo cual representa a la **función de cifrado o una transformación de cifrado.**

El proceso de aplicar la transformación de E_k a un mensaje m que pertenece a M es usualmente nombrado **cifrado de m** (cifrado del mensaje en claro). En conclusión la siguiente notación expresa el proceso que se lleva a cabo al realizar el cifrado de m.

$$\text{Cifrado } E_{k1}(M) = C$$

DECIFRADO

Definición.- El texto cifrado es transformado en el texto original (texto en claro) utilizando un algoritmo criptográfico y una llave.[11]

Más formalmente podemos decir que para cada elemento de $k_2 \in K$, donde D_{k2} denota una biyección de C a M la cual representa a la **función de decifrado o transformación de decifrado.**

El proceso de aplicar la trasformación D_{k2} a un texto cifrado c es nombrado como el **decifrado de c.**La siguiente notación expresa el proceso que se lleva acabo al realizar el decifrado a c.

$$\text{Decifrado } D_{k2}(C) = M$$

El siguiente diagrama esquematiza gráficamente el proceso.(Fig.1)

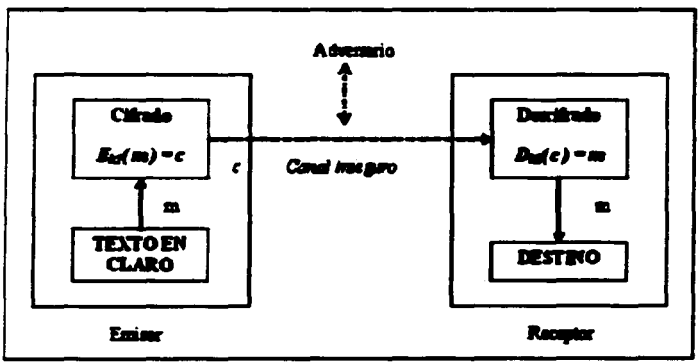


Fig.1

Cabe señalar que un esquema de cifrado consiste de un conjunto dado por E_{k1} : donde $k_1 \in K$ del proceso de transformación de cifrado y el correspondiente al conjunto de D_{k2} : donde $K_2 \in K$ del proceso de transformación de decifrado con la propiedad de que cada elemento de $k_1 \in$ K es la única llave $k_2 \in$ K tal que $D_{k2} = E_{k1}^{-1}$.

Desde el punto de vista del cifrado y decifrado de un mensaje la recuperación del mensaje en claro debe cumplir con la siguiente identidad :

$$D_{k2}(E_{k1}(M)) = M \text{ para toda } m \in M$$

Las llaves k_1 y k_2 en la anterior definición son nombradas como un **par de llaves** y en ocasiones es denotado como (k_1, k_2), hay que tener en cuenta que puede darse el caso de que $k_1 = k_2$ más adelante se explicarán los tipos de esquemas de llaves.

2.4. Componentes de un Cifrado

Algoritmo de Cifrado.- Es la función matemática que realiza la tarea de cifrado de datos y decifrado.[12]

Llaves de Cifrado.- Las llaves de cifrado son las que se utilizan para poder cifrar un mensaje en claro y que mantendrán la confidencialidad del mensaje, así podra ser utilizada para decifrar el mensaje cifrado y obtener en mensaje en claro.[12]

Longitud de Llave.- La longitud de la llave la determinará el algoritmo que utilicemos para cifrar nuestro mensaje en claro , cabe señalar que entre mayor sea la longitud de la llave está será más fuerte y por consecuencia más dificil de romperse.[12]

Texto en Claro.- Se refiere aquella información que deseemos cifrar.[12]

Texto Cifrado.- Es el texto obtenido después de realizar la transformación al texto en claro.[12]

2.5. Participantes en la Comunicación

A continuación definiremos los participantes que intervienen en una comunicacion :

+ Una *entidad* es alguien o algo que envía, recibe o manipula la información, sean Alice y Bob entidades y una entidad es una persona o una terminal de la computadora.
+ Un *emisor* es una entidad entre una comunicación entre dos partes el cual es el legitimo transmisor de la información.
+ Un *receptor* es una entidad en una comunicación entre dos partes el cual tiene la intención de recibir la información.
+ Un *adversario* es una entidad en una comunicación entre dos partes el cual no es el emisor ni el receptor y él cual trata de ganar la información proveida entre el emisor y el receptor. Un adversario frecuentemente pensara jugar el rol tanto de legitimo emisor o receptor.

2.5.1. Canales

:: Un canal es un intento de llevar información de una entidad a otra.

:: Un canal físicamente seguro o canal seguro es aquel tal que no existe un acceso físico al adversario.

:: Un canal inseguro es uno tal que para las partes distintas a estas la información es expuesta a borrado, modificación y lectura de la misma.

:: Un canal seguro es uno para el cual un adversario no tiene la habilidad para borrar, modificar y leer la información.

2.6. Técnicas Criptográficas

Una técnica criptográfica , es también conocida como cifrado, es la función matemática usada para cifrar y decifrar. Existen dos tipos de técnicas criptográficas que son utilizadas en la actualidad y una tercera que combina las dos técnicas anteriores.

:: Cifrado simétrico.

:: Cifrado asimétrico.

:: Cifrado Híbrido Público/Privado.

2.7. Consiguiendo Confidencialidad

Un esquema de cifrado puede ser utilizado con el proposito de conseguir confidencialidad, entre las 2 partes Alice y Bob en un principio realizan secretamente un intercambio de par de llaves ($k1$, $k2$). En un subsecuente instante de tiempo, Alice desea enviarle un mensaje m tal que ϵ M a Bob.

Alice calcúla $c = E_{k1}(m)$ y se lo envía a Bob, cuando Bob recibe c calcúla $D_{k2}(c)$ y de aquí recobra el mensaje original m.

La pregunta obligada surge en el por qué? es necesario las llaves, por que no únicamente seleccionar un cifrado y su correspondiente función de decifrado. Teniendo transformaciones las cuales son muy similares entre si pero caracterizadas por llaves, alguna transformación en particular uno no debe de rediseñar el esquema completamente únicamente se debe cambiar la llave, el cambio frecuente de la llave representa una práctica sana de seguridad.

Como analogía consideremos una caja fuerte con su propia cerradura de seguridad a través de una combinación. La estructura de la cerradura se encuentra disponible a cualquiera que desee comprarla pero la combinación es elegida y colocada por el propietario. Si el propietario sospecha de que la combinación ha sido revelada el puede fácilmente cambiar la combinación sin cambiar físicamente el mecanismo.

2.8. Cifrado Simétrico

Las caracteristica de este tipo de algoritmo están plasmadas en la utilización de la llave, donde la llave utilizada para realizar el cifrado puede ser calculada con la misma llave para decifrar pudiendo notar que la llave es la misma para realizar el método de cifrado y decifrado.

Este algorimo también llamado algoritmo de llave privada, algoritmo de única llave, requiere que el Emisor y el Receptor realicen el acuerdo de llave antes de comenzar la comunicación vía red. La seguridad del algoritmo simétrico recae sobre la llave, divulgando la llave significa que cualquiera pudiera cifrar y decifrar el mensaje. Por lo tanto la llave debe de permanecer en secreto.[11]

$$\text{Cifrado } E_k(M) = C$$
$$\text{Decifrado } D_k(C) = M$$

2.8.1. Cifrado de César

Consideremos un esquema de cifrado que consiste de un conjunto de transformaciones para cifrar y decifrar sean E_{k1} : donde $k1 \in K$ y D_{k2} : donde $k2 \in K$ respectivamente, recordemos que K es el espacio de llave.

El esquema de cifrado es considerado de llave simetrica si para cada asociada par de llaves (k1 , k2) cifrado/decifrado es computacionalmente fácil determinar k2 conociendo únicamente k1 y para determinar k1 a partir de k2, es decir, que se cumpla que $k1 = k2$

En más esquemas de cifrado de llave simetrica el término llega a ser apropiado; otro término utilizado en la literatura es el llamado llave-única, llave-privada.

Veamos ahora un ejemplo que ilustre lo mencionado anteriormente. Sea el conjunto A = {A, B, C . . . . . Z} al conjunto que contiene el alfabeto del español, donde M y C son el conjunto de todas las cadenas de longitud cinco sobre el conjunto A. La llave k1 es escogida para ser una permutación en grupos cada uno teniendo 5 letras (en caso de que la longitud del mensaje no sea multiplo de 5 colocamos ceros de relleno y que no altere su significado real), y una permutación k1 es aplicada para cada letra una a la vez. Para decifrar, la permutación inversa es $k2 = k1^{-1}$ es aplicada a cada letra del texto cifrado.

Cifrado César

Supongamos que la llave k1 es elegida para ser la permutación la cual mapea cada letra del alfabeto tres posiciones a la derecha como se muestra en la siguiente expresión :

$$k1 = \begin{matrix} A & B & C & \ldots\ldots\ldots & Z \\ D & E & F & \ldots\ldots\ldots & C \end{matrix}$$

Y teniendo el siguiente mensaje :

Mensaje en Claro = mensaje secreto de cesar
Mensaje Cifrado = PHQVDMH VHFUWHR GH FHVDU

Donde las dos parte se comunican utilizando el cifrado de llave simétrico, el cual podrá ser decifrado por el siguiente diagrama(Fig.2) :

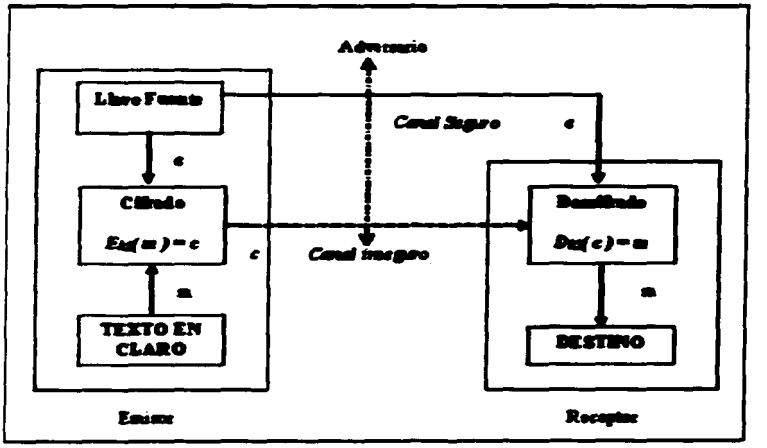


Fig.2

Uno de los mejores usos con el sistema de llave simétrica es el encontrar un método eficiente para realizar un acuerdo sobre el intercambio de llaves seguro, este problema es considerado como el problema de distribución de llave.

Hasta el momento, asumimos que las partes conocen el conjunto de transformaciones de cifrado y decifrado, es decir, conocen todos los esquemas de cifrado, sabemos bien que la única información que debe ser mantenida en secreto es la llave k2 pero en el cifrado de llave simétrico la llave k1 debe también ser mantenida en secreto debido a que a partir de la llave k2 puede ser deducida a partir de la llave k1.

Dentro del esquema de llave simétrico se destacan dos tipos importantes :

:: Cifrado por Bloque.

:: Cifrado por Flujo.

2.8.2. Cifrado por Bloque

Un cifrado de bloque es un esquema de cifrado que particiona el texto en claro para ser transmitido en cadenas llamadas bloques de longitud fija llamada t sobre el alfabeto A y va cifrando un bloque a la vez.[9]

Existen dos clases importantes de cifrado por bloque los cuales son el **cifrado por sustitución y el cifrado por transposición** , así como el **cifrado de producto** que combina los dos anteriores.

2.8.3. Cifrado por Sustitución Simple

Sea el conjunto A del alfabeto con q símbolos y donde M es el conjunto de cadenas de longitud t sobre el conjunto A.Sea K el conjunto de todas las permutaciones sobre el conjunto A, definimos para cada $k1 \in K$ una transformación de cifrado E_{k1} como :

$$E_{k1} = (k1(m1)\ k1(m2) \ldots\ldots k1(mt)) = (c1\ c2 \ldots\ldots ct).$$

Donde m = (m1 m2 ..... $mt \in M$). En otras palabras para cada símbolo en t-tuplas sustituye este por otro símbolo del conjunto A acorde a alguna permutación fija de k1. Para decifrar tenemos que c = (c1 c2 ..... ct) realizamos el cálculo de la permutación inversa teniendo que $k2 = k1^{-1}$ y por lo tanto :

$$D_{k2} = (k2(c1)\ k2(c2) \ldots k2(ct)) = (m1\ m2 \ldots\ldots mt) = m$$

Donde E_{k1} es llamado cifrado de sustitución o cifrado de sustitución monoalfabetico y donde el número de las distintas combinaciones del cifrado de sustitución es q! y es independiente del tamaño del bloque.

Cabe recalcar que el cifrado de sustitución simple aplicado a bloques de tamaño pequeño provee una inadecuada seguridad de igual forma comparado cuando el espacio de llaves es extremadamente extenso.

Cabe observar que se presenta una vulnerabilidad en este esquema debido a que la distrubución de frecuencia de letras se conserva en el texto cifrado por ejemplo la letra *e* ocurre más frecuentemente que las demás letras del alfabeto, en base a esto en una secuencia de bloques en el texto cifrado es probable que corresponda la letra *e* en el correspondiente texto en claro , por lo que analizando una cierta cantidad de bloques del texto cifrado un cripotoanalista podría determinar la llave.[8]

2.8.4. Cifrado de Sustitución Homofónico

Sea el conjunto A del alfabeto y para cada símbolo $a \in A$ se le asocia a un conjunto A(a) de cadenas de t símbolos, con la restricción de que los conjuntos A(a) y a $\in$ A son parejas disjuntas, donde un cifrado de sustitución homofónico remplaza cada símbolo de bloque en texto en claro por una cadena aleatoria tomada de A(a).

En el proceso inverso para decifrar una cadena c con t símbolos, uno debe determinar un elemento en en a $\in$ A tal que $c \in$ A(a). Debemos de tener en cuenta que la llave para el cifrado se encuentra sobre el conjunto A(a).

Consideremos el conjunto A formado por los siguientes elementos {a,b} y al conjunto A(a) = { 00, 01 } de igual manera al conjunto A(b) = { 01 , 11 }.

Consideremos un bloque de mensaje en claro como **ab** una de las posibilidades de cifrado sería **0001 , 0011 , *1001* , 1011**. Obsevamos que el codominio de la función de 4 elementos es :

aa –>{ 0000,0010,1000,1010 }
ab –>{ 0001,0011,1001,1011 }
ba –>{ 0100,0110,1100,1110 }
bb –>{ 0101,0111,1101,1111 }

Donde una cadena de 4 bits de longitud únicamente identifica un elemento del codominio y por lo tanto un mensaje en texto en claro.

A menudo los símbolos no ocurren con igual frecuencia en el texto en claro como se presenta en el cifrado de sustitución simple que presentaba una frecuencia de símbolos no uniforme. Un cifrado homofónico tiene la característica que la frecuencia de ocurrencia de símbolos en el texto cifrado se presenta más uniforme reflejándose como la expansión de los datos.

2.8.5. Cifrado de Sustitución Polialfabetico

Un cifrado de sustitución polialfabetico es un cifrado por bloques, donde cada bloque tiene una longitud t sobre un alfabeto A y tiene las siguientes propiedades :

:: El espacio de la llave k consiste de todos los conjuntos ordenados en t permutaciones (p1 , p2 , ... pt) donde cada permutación p_i esta definida para el conjunto A.

:: El cifrado del mensaje m = (m1 m2 .... mt) en función de la llave k1 = (p1 , p2 .... pt) se define como E_{k1} = (p1(m1) p2(m2) ..... pt(mt)).

:: El decifrado asociado con la llave k1 = (p1 , p2 .... pt) esta definido como k2 = ($p1^{-1}$, $p2^{-1}$ ..... pt^{-1}).

Una vez establecidas las caracteristicas del cifrado por sustitución alfabetico veamos un ejemplo de este tipo cifrado como lo es el **cifrado vigenére** que acontinuación explicaremos.

Cifrado de Vigenére

Definamos al conjunto A = { A , B , C .... Z} y a t = 3 , una vez definido esto elegimos a k1 = (p1 , p2 , p3) donde p1 queda definida para mapear cada letra hacia 3 posiciones a la derecha con respecto al alfabeto, p2 queda definida para mapear cada letra 7 posiciones a la derecha y p3 queda definida para mapear 10 posiciones a la derecha.[8]

Sea el siguiente mensaje :

m = THIS CIPHER IS CERTAINLY NOT SECURE.

Aplicando el cifrado de vigenére como lo definimos anteriormente tendríamos lo siguiente :

c = E_e(m) = WOSV JSSOOU PC FLBWHSQSI QVD VLMXYO.

Podemos notar que el cifrado polialfabetico tiene la ventaja sobre el cifrado de sustitución simple donde la frecuencia de los símbolos del alfabeto no se conserva un ejemplo claro lo vemos en el símbolo E que toma distintos valor como lo son el símbolo O y L.

Sin embargo el cifrado polialfabetico no es significativamente más dificil de criptoanalizar, debido a que las letras del texto cifrado pueden ser divididas en t grupos (donde el grupo i esta definido para 1 <= i <= t utilizando permutaciones de p_i) y un análisis de frecuencia se puede efectuar sobre cada grupo.

2.8.6. Cifrado por Tranposición

Otra clase de cifrado de llave-simétrica es el cifrado por transposición simple, el cual únicamente permuta los símbolos en un bloque.

Consideremos un cifrado simétrico por bloque, con bloques de longitud t. Donde K es el conjunto de todas las permutaciones sobre el conjunto definido por { 1 , 2 ,3 .... t }, para cada $k_1 \in K$ definimos a la función de cifrado como :

$$E_{k1}(\mathrm{m}) = (m_{k1}(1)m_{k1}(2) \ldots\ldots m_{k1}(t)).$$

Donde sabemos que m = (m1 m2 ... mt) $\in M$ el espacio del mensaje , por lo que el conjunto de todas las transformaciones es llamado cifrado de transposición simple.

El decifrado correspondiente a la llave k_1 es la permutación inversa tal que $k_2 = k1_{-1}$ por lo que para decifrar a c = (c1 c2 ... ct) calculamos :

$$D_{k2}(\mathrm{c}) = (c_{k2}(1)c_{k2}(2) \ldots\ldots c_{k2}(t)).$$

Observamos que un cifrado de transposición simple preserva el número de símbolos de un tipo de dato dentro de un bloque por tal razón es facilmente de ser criptoanalizado.

2.8.7. Cifrado de Composición y Producto

En el orden de describir un cifrado de producto, el concepto de composición de funciones es introducido por tal motivo.

Composición es un camino conveniente de construir más complicadas funciones de una más simple, a continuación definiremos el concepto de *composición de función* más detalladamente.

Composición de Función

Sean S , T y U conjuntos finitos y definamos las siguientes funciones f: S –>T y g: T–>U. La composición de g con f , denotada como **g o f** o simplemente **g f**, es una función de S a U como se puede ver en la siguiente figura(Fig.3) :

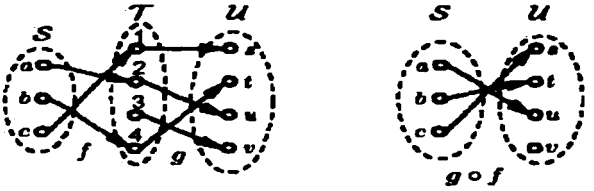


Fig.3

La composición puede ser facilmente extendida a más de 2 funciones como por ejemplo para f1, f2 , ... ft uno podría definir ft o .... f2 o f1 con la restricción de que el dominio de ft sea igual al codominio de ft-1 y así sucesivamente.

Cifrado de Producto

La sustitución simple y cifrado de transposición individualmente como hemos visto no proveen un alto nivel de seguridad. Sin embargo, si combinamos estos dos tipos de transformaciones es posible obener un cifrado fuerte.

Un ejemplo del cifrado de producto es una composición de t >= 2 transformaciones E_{k1} E_{k2} .... E_{kt} donde para cada E_{ki} , 1 <= i <= t puede ser tanto un cifrado de sustitución o un cifrado de transposición, para su mejor manejo entenderemos a la composición de una sustitución y una transposición como una **ronda**.

Daremos a continuación un ejemplo :

Sea $M = C = K$ donde son el conjunto de todas las cadenas binarias de longitud 6, el número de elementos en M es $2^6 = 64$.

Sea m definido como m = (m1 m2 ... m6) y definimos que :

$E_{k1}^{(1)}$ = m + k donde k ∈ K.

$E^{(2)}$ = (m4 m5 m6 m1 m2 m3).

Donde + representa a la OR- exclusiva (XOR), recordando se encuentra definica como :

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 1 = 0$$

Observamos que $E_{k1}^{(1)}$ define a un cifrado de sustitución polialfabetico y que $E^{(2)}$ define a un cifrado de transposición en el cual no se definio ninguna llave para este caso en particular, por lo que el producto de $E_{k1}^{(1)}$ $E^{(2)}$ corresponde a una ronda.

2.8.8. Confusión y Difusión

Una sustitución en una ronda la consideraremos para añadir confusión al proceso de cifrado ya que una transposición añade difusión.

La confusión tiene como intención hacer la relación entre la llave y el texto cifrado tan compleja como sea posible mientras que la difusión se refiere a extender los bits en el mensaje así que si existe alguna redundancia en el texto en claro es extendida sobre el texto cifrado.

Por lo que una ronda puede añadir tanto una confusión y difusión en el cifrado, en los modernos sistemas de cifrado de bloque se aplican un número de rondas en sucesiones para cifrar el texto en claro.

2.8.9. Cifrado por Flujo

El cifrado de flujo forma una clase importante de esquema de cifrado de llave simétrico, es en esencia un cifrado de bloque simple , es decir, bloques de longitud igual a 1.

Qué hace a esto útil?

El factor de cifrado de transformación puede cambiar para cada símbolo en el texto en claro, en la sustitución donde la transmisión de error es altamente probable, el cifrado por flujo presenta una ventaja ya que no presenta un error de propagación porque únicamente se trabaja sobre un símbolo y no sobre un bloque como en el caso del cifrado por bloque donde su propagación del error es muy alta.

Definamos formalmente el Cifrado por Flujo.

Sea K el espacio de llave para un conjunto de cifrados de transformación y una secuencia de símbolos e1 e2 .... ei ϵ K la cual es llamada una cadena de llaves.

Definamos al conjunto A del alfabeto con q símbolos y sea E_{k1} un cifrado de sustitución simple con bloques de longitud 1 donde k1 ϵ K.

También definamos a m1 m2 m3 ... como una cadena de texto en claro y a e1 e2 e3 ... a un flujo de llaves de K, un cifrado por flujo toma la cadena del texto en claro y produce una cadena de texto cifrado c1 c2 c3 .... donde $c_i = E_{k1i}(m_i)$.

Si k_{2i} denota la inversa de k_{1i} entonces $D_{k2i}(c_i) = m_i$.

Un cifrado de flujo aplica un cifrado simple acorde al flujo de llaves utilizadas, el flujo de llaves puede ser generado de manera aleatoria o por un algoritmo el cual genera el flujo de llaves de una llave inicial o semilla, tal algoritmo es llamado generador de flujo de llaves.

2.8.10. Cifrado de Vernam

El factor de motivación del cifrado de vernam fue su simplicidad y lo fácil de implementar.

El cifrado de Vernam es un cifrado de flujo definido sobre el alfabeto A ={ 0, 1} y definiendo los siguientes componentes :

:: Un mensaje binario definido como m1, m2 , ... mt.

:: Una cadena de llaves binarias $k_1, k_2 \ldots, k_t$, de una misma longitud que la cadena de texto cifrado.

:: Cadena de texto cifrado c1, c2 ... ct donde :

$$c_i = m_i + k_i \quad 1 <= i <= t.$$

Si la cadena de llaves es escogida aleatoriamente y nunca es utilizada nuevamente dicha cadena, entonces el sistema es conocido como **one-time o one-time pad**.[9]

Para ver el funcionamiento del cifrado de Vernam observamos que son 2 cifrados de sustitución sobre el conjunto A, uno de los cifrados simplemente mapea la identidad definida como E_0 el cual envía 0 a 0 y 1 a 1, el otro cifrado definido como E_1 envía 0 a 1 y 1 a 0. Cuando el flujo de llaves contiene a un 0 aplica E_0 para el correspondiente símbolo del texto en claro; en el otro caso aplica E_1.

Como ya mencionamos anteriormente la cadena de llaves es elegida aleatoriamentes y utilizada sólo una vez en caso de que sea reutilizada existen caminos para que el sistema sea atacado. Por ejemplo si c1 c2 ... ct y sea c1' c2' ... ct' son dos cadenas de texto cifrado producidas poe el mismo flujo de llave $k_1 k_2 \ldots k_t$ entonces :

$c_i = m_1 + k_i$ así como

$c'_i = m'_1 + k'_i$ por lo tanto

$c_i + c'_i = m_1 + m'_1$ Por lo que la redundancia en las letras puede permitir el criptoanálisis.

One-time pad

Para entender un poco más del término de **one-time pad** podemos entender que teoricamente es irrompible, esto es que si un criptoanalista tiene una cadena de texto cifrado c1 c2 ... ct utilizando una llave aleatoria la cual ha sido utilizada únicamenete sólo una vez el criptoanalista sólo podrá creer que el texto en claro es una cadena binaria de longitud t, es decir, cadenas binarias de t-bits que son igualmente probables en el texto en claro.

2.9. Espacio de Llave

El tamaño del espacio de la llave es el número de par de llaves para el cifrado/decifrado que esta disponible en el sistema de cifrado.

Una llave es típicamente un camino compacto para especificar la transformación del cifrado. Por ejemplo un cifrado de transposición de bloque con una longitud t tiene $t!$ funciones del cifrado de las cuales escoger.

Cada una puede ser simplemente descrita por una permutación la cual es llamada llave. Es importante relacionar la seguridad del esquema de cifrado con respecto al tamaño del espacio de la llave el cual consiste en que el espacio de llave sea lo suficientemente grande para imposibilitar una búsqueda exhaustiva.

2.10. Autenticación

Autenticación es un término que es usado y frecuentemente abusado en un amplio sentido.

Cuando se establece una comunicación entre las dos partes se debe de garantizar que las entidades son quien dicen ser, o que la información no ha sido manipulada por partes no autorizadas. La autenticación es una parte específica como objetivo de la seguridad la cual se trata de conseguir.

La autenticación es uno de los objetivos más importantes de la seguridad. Hasta mediados de los años 70's fue generalmente creido que el secreto y la autenticación eran intrinsecamente conectadas. Con el descubrimiento de las funciones hash y las firmas digitales se observó que el secreto y la autenticación se encontraban verdaderamente separadas y independientemente dentro de los objetivos de la seguridad.

Podríamos pensar que no es de mucha importancia el separar uno del otro pero es evidente que es esencial, por ejemplo si existe una comunicación entre 2 entidades Alice y Bob supongamos que cuando Alice se encuentra en un país y Bob se encuentra en otro país distinto al de Alice, quizas algún país no permitiera la privacidad o secreto sobre sus canales ; uno o ambos pai-ses pudieran desear tener la habilidad para monitorear toda la comunicación en el canal.

Alice y Bob, sin embargo, les gustaría estar seguros de la identidad del otro, y de la integridad y origen de la información que entre ellos se envían y reciben. El anterior escenario ilustra aspectos independientes de la necesidad de la autenticación, estas dos posilibidades son a considerar :

1. A y B pudieran estar comunicándose con un retardo no apropiado de tiempo. Esto es, ellos están ambos activos en la comunicación en tiempo real.

2. A y B pudieran estar cambiando un mensaje con un retardo de tiempo. Esto es, el mensaje puede ser ruteado por varias redes, almacenando y enviando en algún tiempo después.

En el primer caso A y B pudieron desear verificar la identidad en tiempo real. Esto puede ser logrado por A enviando a B una contraseña para la cual B es la única entidad que puede responder correctamente. Bob pudiera ejecutar una acción similar para identificar a Alice. Este tipo de autenticación es comunmente referida como *autenticación de entidad o simplemente identificación.*

Para el segundo caso, no es conveniente el uso de la contraseña y esperar la respuesta además la ruta de comunicación que se da puede ser únicamente en una dirección. Diferentes técnicas son ahora requeridas para autenticar el originador del mensaje. Esta forma de autenticación es llamada *autenticación del origen de los datos.*

2.10.1. Identificación

Una identificación o técnica de autenticación de entidad asegura una parte para la adquisición de corroboración de evidencias de ambas entidades y de una de una segunda parte implicada, donde esta última fue activada en el momento en que la evidencia fue creada o adquirida. Tipicamente los datos transmitidos es lo único que es necesario para identificar la comunicación, de las partes. Las entidades son ambas activadas en la comunicación.

Ejemplo de lo mencionado anteriormente, A llama a B por teléfono si A y B se conocen uno al otro la entidad de autenticación es proveida por el reconocimiento de la voz.

Otro ejemplo, una persona A provee a una máquina bancaria un número de identificación personal PID junto con una tarjeta de débito que contiene información sobre A. La máquina utiliza la información de la tarjeta y el PID para verificar la identidad del poseedor de la tarjeta. Si la verificación resulta exitosa a la persona A se le da el acceso a varios servicios ofrecidos por la máquina.

2.10.2. Autenticación del Origen de los Datos

La técnica de autenticación provee para alguna de las partes que recibe un mensaje, asegurar (para corroborar evidencias) la identidad que originó el mensaje.

Frecuentemente un mensaje es proporcionado a B junto con una información adicional que B puede determinar la identidad que originó el mensaje. Esta forma de autenticación tipicamente no proporciona una garantía, pero es útil en situaciones donde una de las partes no se encuentra activa en la comunicación.

2.11. Cifrado Asimétrico

También conocido como algoritmo de llave pública el cual es diseñado para que la llave utilizada para el cifrado sea diferente de la llave utilizada para decifrar. Además, la llave de decifrado no podría ser calculada por la llave de cifrado.

El algoritmo es llamado de **llave pública** porque la llave de cifrado puede ser pública al mundo, donde un extraño pudiera utilizar la llave pública para cifrar un mensaje, pero únicamente una persona específica podrá decifrar con la llave privada.

Podemos distinguir dos aspectos importantes , el primero que existen dos llaves en este esquema donde se conocerá como **llave pública** a la llave utilizada para cifrar y segundo se conocerá como **llave privada** a la llave utilizada para realizar el decifrado.

Cifrado E_k(M) = C Donde k es la llave pública
Decifrado D_k(C) = M Donde k es la llave privada

Definición Formal

Sea { E_{k1} : donde $k1 \in K$ } un conjunto de transformaciones de cifrado y sea { D_{k2} : donde $k2 \in K$ } un conjunto de correspondientes transformaciones de decifrado, donde K es el conjunto del espacio de la llave.

Consideremos un par asociado a transformaciones de cifrado y decifrado (E_{k1} , D_{k2}) y supongamos que cada par tiene la propiedad que conociendo E_{k1} es computacionalmente idecidible dado un texto cifrado aleatorio donde $c \in C$ poder encontrar el mensaje $m \in M$ tal que E_{k1}(m) = c. Esta propiedad implica que dada k1 es poco probable determinar la correspondiente llave del decifrado k2, por supuesto k1 y k2 simplemente describen las funciones de cifrar y decifrar respectivamente.

Supongamos la comunicación entre las dos partes Alice(emisor) y Bob(receptor) como se observa en la siguiente figura(Fig.4) :

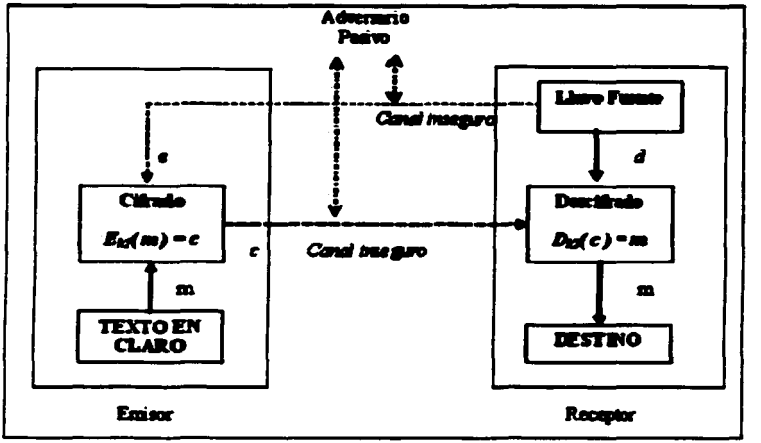


Fig.4

Bob selecciona un par de llaves (k_1 , k_2), Bob envía la llave de cifrado k_1 llamada la llave pública a Alice sobre el canal pero guardando en secreto la llave de decifrado k_2 llamada llave privada.

Alice pude subsecuentemente enviar un mensaje a Bob para aplicar la transformación de cifrado determinada por la llave pública de Bob, para obtener $c = E_{k1}(m)$ Bob decifra el texto cifrado c aplicando la transformación inversa D_{k2} únicamente determinada por la llave k_2.

Debemos notar que en la figura que la llave de cifrado es transmitida a Alice sobre un canal inseguro, este canal inseguro puede ser el mismo canal sobre el cual el texto cifrado esta siendo transmitido. Posteriormente la llave de cifrado k_1 no requiere ser guardada en secreto, esta puede ser hecha pública.

Alguna entidad puede subsecuentemente enviar un mensaje cifrado a Bob el cual únicamente él podrá decifrar. En la siguiente figura(Fig.5) se ilustra la idea donde A_1, A_2 y A_3 son distintas entidades, debemos notar que si la entidad A_1 destruye el mensaje m_1 después de cifrarlo obteniendo c_1 entonces la entidad A_1 no podrá recobrar m_1 de c_1.

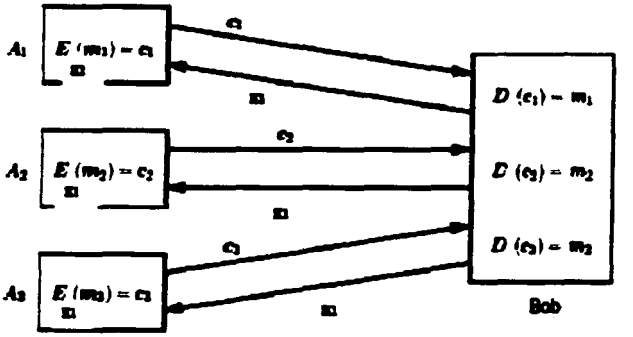


Fig.5

Como una analogía, consideremos una caja metálica con una tapa de seguridad que tiene una combinación que únicamente el dueño podrá conocer. Si la cerradura es abierta y hecha públicamente disponible, entonces alguien puede colocar un mensaje dentro de la caja y solamente el dueño de la caja podrá recobrar el mensaje. De igual manera la entidad que colocó el mensaje en la caja no esta habilitado para recuperarlo.

El cifrado de llave pública, asume del conocimiento de la llave pública k_1 no permite calcular la llave privada k_2.

Definición

Consideremos un esquema de cifrado conformado por un conjunto de transformaciones de cifrado y decifrado definidas como $\{ E_{k1}$: donde $k1 \in K \}$ y $\{ D_{k2}$: donde $k_2 \in K \}$ respectivamennte. El método de cifrado es un esquema de cifrado de llave pública dado que para cada par (k_1, k_2) existe una llave k_1 (la llave pública) es hecha públicamente disponible, mientras que k_2 (llave privada) es guardada en secreto.[8]

Para que el esquema sea seguro, debe ser computacionalmente indecidible calcular k_2 de k_1.

2.12. Cifrado Híbrido Público / Privado

Como ya vimos los dos clásicos algoritmos de cifrado que se utilizan, donde el algoritmo de llave privada por lo general es utilizado para la protección de la información almacenada en disco duro , o para cifrar la información que se envía entre dos distintos equipos.

Mientras que el algorritmo de llave pública generalmente es utilizado para generar firmas digitales sobre correos electronicos, certificados,etc.

El algoritmo híbrido que mezcla tanto la ideología de llave pública como el de llave privada; donde el algoritmo de llave pública es utilizado para el intercambio de una llave de sesión lo cual es usado como base del algoritmo de llave privada.

Cabe mencionar que una llave de sesión es utilizada por una sola sesión de cifrado y posteriormente es desechada.Casi todas las implementaciones de llave pública son actualmente algoritmos híbridos.

2.13. Algoritmos de Llave Privada

Crypt

Es el programa original de UNIX que fue modelado sobre la máquina de cifrado de German Enigma, crypt utiliza una longitud variable en su llave, algunos programas pueden automaticamente decifrar archivos sin conocer a priori la llave que se le aplicó al texto en claro. Es claro entonces que crypto no es seguro.

DES

Data Encryption Standard , desarrollado en el año de 1970 por la National Bureau of Standards and Technology que posteriormente fue renombrada NIST [7] y junto con IBM. DES utiliza una longitud de llave de 56-bits.

RC5

Es un cifrado por bloque desarrollado por Ronald Rivest y fue publicado en el año de 1994, RC5 permite definir la longitud de la llave, el tamaño de los bloques de los datos y el número de rondas de cifrado.

IDEA

[7] National Institute of Standards and Technology

International Data Encryption Algorithm, desarrollado en Zurich, desarrollado por James L. Massey y Xuejia Lai el cual fue publicado en el año de 1990. IDEA utiliza una longitud de llave de 128-bits.

Skipjack

Es un algoritmo clasificado , desarrollado por la National Security Agency NSA, se requiere de una acreditación para poder revisar su código fuente y especificaciones de diseño. Skipjack utiliza una longitud de llave de 80 bits fue usado para un chip denominado Clipper.

2.14. Algoritmos de Llave Pública

Diffie-Hellman

Es el parte aguas de lo que hoy se conoce como algoritmo de llave pública, es un sistema criptográfico de intercambio de llave, Diffie-Hellman actualmente no es un método de cifrado y decifrado pero si implicó un método de desarrollo y intercambio sobre una llave compartida sobre el canal público de comunicación.

Entre las dos partes (emisor y receptor) deben de realizar el acuerdo sobre un valor numérico con el cual cada parte podrá calcular su llave, transformaciones matemáticas se aplican a las llaves que son intercambiadas.

RSA

El mejor conocido sistema criptográfico de llave pública desarrollado por los profesores de MIT Ronal Rivest y Adi Shamir, así como también por el profesor de USC Leonard Adleman, propio el nombre del algoritmo a las siglas de los creadores.

RSA puede ser usado en dos sentidos para el cifrado de información así como las bases de un sistema de firmas digitales. Las firmas digitales son utilizadas pora proteger autoría y la autenticidad de la información digital. En cuanto a referencia de la longitud de la llave esta puede ser variable dependerá sobre la aplicación en particular ; entre mayor sea la longitud es considerado más segura.

El Gamal

Es otro algoritmo que se basa en la exponenciación y aritmética modular. El Gamal es utilizado al igual que el algoritmo de RSA para el cifrado y firmas digitales.

DSA

Algoritmo de Firmas Digitales [8] desarrollado por la NSA y adoptado como estándar por la NIST. DSA utiliza una longitud variable de llave oscilando entre los 512 y 1024 bits, el algoritmo es diseñado especificamente para realizar firmas digitales pero también es posible su utilización para el cifrado de texto.

El DSA también nombrado DSS, de la misma manera de que DEA es usualmente para DES.

2.15. Simétrico vs Antisimetrico

El esquema de *llave simetrica* y el de *llave pública* presentan algunas ventajas y desventajas en relación uno con otro, algunas de las cuales son comunes para ambos esquemas.

Los sistemas criptográficos actuales explotan la fuerza de cada uno de los esquemas, el cifrado de los datos frecuentemete representa el mayor tiempo consumido en el preceso de cifrar. El esquema de llave pública para poder establecer la llave toma una pequeña fracción de tiempo en el proceso total del cifrado entre la entidad A y B.

A la fecha, la ejecución computacional de un cifrado de llave pública es inferior a el total de cifrado de llave simetrica, aunque esto aún no se ha probado. Los puntos importantes que hay que destacar son lo siguientes:

:: El esquema de llave pública facilita la eficiencia de las firmas (particularmente para el No-Repudio) y el manejo de llave.

:: El esquema de llave simetrica es eficiente para el cifrado y algunas aplicaciones de integridad de datos.

Observación

Para evitar ambiguedad, una convención utilizada para nombrar el término de llave privada en asociación con el esquema de llave pública, y la llave secreta en asociación con el esquema de llave simétrica. Esto puede ser motivante por la siguiente línea de reflexión ; existen 2 o más partes que comparten un secreto pero una llave es exactamente privada cuando únicamente un parte conoce a esta.

Estos son algunos esquemas conocidos, donde se cree que es seguro el esquema de cifrado de llave pública, pero no ha sido matemáticamente probado. Esto no se presenta en el esquema de llave simétrica donde únicamente el sistema que ha sido probado que es seguro es el *one-time pad*.

[8] Digital Signature Algorithm

2.15.1. Ventajas - Llave Simetrica

:: El cifrado de llave simetrica puede ser diseñado para tener una alta proporción de datos. Algunas implementaciones de hardware consiguen cifrar proporciones de cientos de megabytes por segundo, mientras que la implementación de software puede obtener una proporción del rango de los megabytes por segundo únicamente.

:: Las llaves para el cifrado de llave simetrica son relativamente cortas.

:: El cifrado de llave simetrica puede ser empleado como primitivas para construir varios mecanismo criptográficos incluyendo el generador de números aleatorios, funciones hash, y esquemas de firmas digitales computacionalmente eficientes.

:: El cifrado de llave simetrica puede ser compuesto para producir cifrados fuertes. Transformaciones simples las cuales son faciles de analizar, pero su propia debilidad puede ser utilizada para construir cifrados producto fuertes.

:: Presenta una historia extensa, que a pesar de las invenciones mucho del conocimiento en esta área ha sido adquirido subsecuentemente para la invención de las computadoras digitales y en particular del diseño del algoritmo DES en los principios de 1970.[8]

2.15.2. Desventajas - Llave Simétrica

:: En la comunicación entre las dos partes, la llave debe permanecer en secreto en ambas entidades.

:: En la comunicación entre las dos partes, la entidad A y B una práctica criptografía sana dicta que la llave sea cambiada frecuentemente y por lo tanto para cada sesión de comunicación.

:: La Firma Digital es conseguida tipicamente a través de un cifrado de llave simetrica requerirá llaves largas para la función pública.[8]

2.15.3. Ventajas - Llave Pública

:: Únicamente la llave privada debe ser guardada en secreto.

:: Dependiendo sobre el modo de uso, tanto la llave privada como la llave pública pueden permanecer sin cambios por largos periodos de tiempo.

:: Algunos esquemas de llave pública producen relativamente eficientes mecanismo de firmas digitales. La llave utilizada describe la función pública de verificación que es típicamente mucho más pequeña que para los cifrados de llave simétrica.

:: En una red extensa, el número de llaves necesarias puede ser considerablemente pequeño en relación al esquema de llave simetrica.[8]

2.15.4. Desventajas - Llave Pública

:: La proporción de los más populares métodos de cifrado de llave pública son algunos ordenes de magnitud menores que los mejores esquemas de llave simetrica.

:: El tamaño de la llave son típicamente mucho más grandes que los requeridos para el cifrado de llave simétrica.

:: La autenticación de la llave pública debe ser garantizada.

:: Los esquemas de llave pública no han sido provados ser seguros (los mismo podría decirse del cifrado por bloques).

:: La criptografía de llave pública no tiene una extensa historia como el cifrado de llave simetrica, siendo únicamente a mediados del años de 1970.[8]

2.16. Firmas Digitales

El proposito de una firma digital es proporcionar una propuesta para una entidad de exigirle identificar un fragmento de información. El proceso de firmar envuelve la transformación del mensaje y algunos secretos de información tomado por la entidad en una etiqueta llamada firma.

Nomenglatura y Construcción

- M es el conjunto de mensajes que pueden ser firmados.
- S es el conjunto de elementos llamados firmas, posiblemente cadenas binarias de longitud fija.
- S_A es una transformación del conjunto de mensajes M para el conjunto de firmas S y es llamado una transformación de firma para una entidad A. La transformación de S_A es guardada en secreto por la entidad A y será utilizado para crear las firmas para los mensajes de M.
- V_A es una transformación de el conjunto que es el producto cartesiano de $M \times S$ que consiste de todos los pares (m , s) donde $m \in M$ y $s \in S$.V_A es llamado una verificación de la transformación para las firmas de A, es públicamente conocido, y es utilizado por otra entidad para verificar la firma creada por la entidad A.

La transformación de S_A y V_A provee un esquema de firma digital para la entidad A, en ocasiones se utiliza el término de mecanismo de firma digital es utilizado.

2.16.1. Esquema de Firmas Digitales

Mostremos un ejemplo del esquema de firmas digitales en base a la nomenglatura definida anteriormente. Sea M = { m1, m2, m3 } y S representados del lado izquierdo de la figura mostrada abajo de la cual se despliega una función de firma S_A con respecto al conjunto M, del lado derecho de la figura (Fig.6) se encuentra la correspondiente verificación la función V_A.

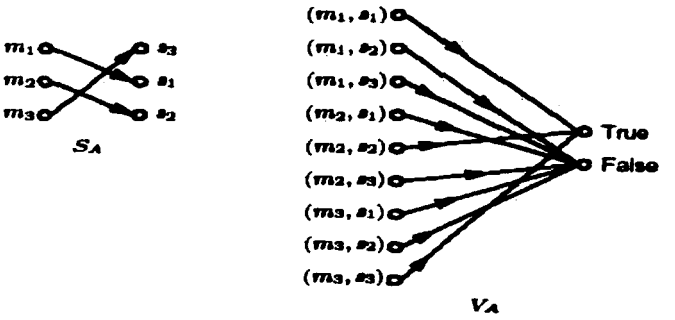


Fig.6

Procedimiento de Firma

La entidad A (el firmante) crea una firma para un mensaje m ϵ M para realizar lo siguiente :

1. Calcular $S = S_A(m)$.
2. Transmitir la pareja (m , s) donde s es llamada la firma del mensaje m.

Proceso de Verificación

Para verificar que una firma s sobre un mensaje m fue creado por la entidad A, una entidad B (el verificador) realiza los siguientes pasos :

1. Obtener la función de verificación V_A de la entidad A.

2. Calcular $u = V_A(\mathrm{m}, \mathrm{s})$.

3. Aceptar la firma creada por la entidad A si el valor de u = verdadero y rechaza la firma si el valor de u = falso.

Propiedades Requeridas para firmar y verificación de funciones

Estas son algunas propiedades que la transformación de firma y verificación deben de satisfacer :

a. S es una firma valida de A sobre el mensaje m si y solo si $V_A(\mathrm{m}, \mathrm{s})$ = verdadero.

b. Es computacionalmente indecidible para alguna entidad que no sea A, encontrar para un mensaje $\mathrm{m} \in M$ y $\mathrm{s} \in S$ talque $V_A(\mathrm{m}, \mathrm{s})$ = verdadero.

En la figura mostrada anteriormente se despliega la propiedad que se marca en el inciso **a.** donde se coloca una flecha si se cumple que V_A de (m_i, s_i) = verdadero , por lo que se coloca la flecha que va de m_i a s_i en el diagrama de S_A. Propiamente para el inciso **b.** se provee la seguridad para que el método y que la firma únicamente ligue a la entidad A con el mensaje que es firmado.

2.16.2. Funciones Hash

Una de las fundamentales primitivas en la criptografía moderna es la criptografía de las funciones hash, algunas veces informalmente llamadas funciones hash one-way.

Definición

Una función hash es computacionalmente eficiente tal que dicha función mapea cadenas binarias de longitud arbitraria a cadenas binarias de longitud fija, que llamaremos valores hash.[9]

Para una función hash cuya producción de valores hash son n-bits, la probabilidad de que una cadena escogida aleatoriamente sea mapeada a un valor hash particular de n-bits (imagen) es 2_{-n}.La idea básica es que el valor hash sirva como una breve representación de una cadena de entrada.

Para hacer uso de la criptografía , una función hash h es típicamente escogida tal que sea computacionalmente indecidible encontrar dos distintas entradas cuyo valor hash sea el mismo , es decir , dos valores de entrada que chocan x y y tal que $h(x) = h(y)$ y que dado un valor hash y específico sea computacionalmente indecidible encontrar una entrada x tal que $h(x) = y$.

El uso común de la función hash son las firmas digitales y también para la integridad de los datos. Con las firmas digitales un mensaje extenso usualmente se le aplica la función hash y únicamente al valor hash es firmado.

La parte que recibe el mensaje verifica que la firma recibida es correcta para el valor hash. Esto ahorra tiempo y espacio comparado a firmar el mensaje directamente, lo que tipicamente traería dividir el mensaje en bloques de apropiado tamaño y firmar cada bloque individualmente.

Debemos notar la capacidad de encontrar dos mensajes con el mismo valor hash el cual es un requerimiento de seguridad, en otro caso la firma sobre un mensaje tiene su valor hash el cual podría ser el mismo como en otro mensaje, permitiendo a un firmante marcar un mensaje y en un instante de tiempo después reclamar haber firmado otro.

Una función hash como ya lo mencionamos anteriormente puede ser utilizada para la integridad de los datos, donde el valos hash corresponde a una particular entrada que es calculada en un instante de tiempo.

La integridad de este valor hash es proteguido de alguna manera, en un subsecuente instante de tiempo, para verificar que los datos de entrada no han sido alterados, el valor hash es recalculado utilizando la entrada que tenemos a la mano, y comparada por igualdad con el valor hash original.

Las aplicaciones de la función hash las enumeraremos a continuación :

I. Protección de virus y distribución de software.

II. Esquemas de firmas digitales y

III. Identificación de Protocolos.

2.17. Criptoanálisis

El punto total que pretende la criptografía es el guardar el texto en claro y la llave en secreto, para protegerse de quien se encuentra escuchando la información que viaja por la red. El término de uso que se le asigna a este tipo de persona será el de adversario, atacante , intruso, entre otras muchos más dentro de la presente tesis utilizaremos por igual alguno de los terminos mencionados anteriormente.

Debemos de tener en mente y presente que el atacante se asume que tiene un completo acceso a la vía de comunicación entre el emisor y receptor.

Entenderemos entonces el Criptoanálisis como la ciencia para recuperar el texto en claro sin tener conocimiento de la llave, lograndolo a través de debilidades que presente el criptosistema lo cual conlleva a la recuperación de la llave, el texto en claro o ambos, por lo que se denomina todo intento de criptoanálisis como un ataque.

Existen distintos tipos de ataques de cripotoanálisis, donde debemos tener conciencia de que el atacante tiene el pleno conocimiento del funcionamiento de los algoritmos criptográficos.A continuación se describiran cada uno de ellos :

I. Únicamente el Texto Cifrado.

II. Conoce el Texto en Claro.

2.17.1. Únicamente el Texto Cifrado

El criptoanalista únicamente tiene en sus manos el texto cifrado de algunos mensaje, todos ellos han sido cifrados con el mismo algoritmo de cifrado.El objetivo principal del criptoanalista es el recobrar el texto en claro o quizas el poder deducir la llave utilizada para cifrar los mensajes.

Lo que tiene el Criptoanalista es :

Mensajes Cifrados. $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$ ..... $C_n = E_k(P_n)$.

Lo que pretende Obtener :

Cualquiera de las dos el Mensaje en claro o la llave.

- $P_1, P_2, \ldots P_n$.
- k.

2.17.2. Conoce el Texto en Claro

El criptoanalista tiene acceso no sólo al texto cifrado sino también al texto en claro de los mensajes. Su trabajo será el poder deducir la llave o llaves utilizadas para cifrar los mensajes o un algoritmo que permita decifrar algun nuevo mensaje cifrado con la misma llave o llaves.

Lo que tiene el Criptoanalista es :

Mensajes Cifrados. $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$ ..... $C_n = E_k(P_n)$.

Lo que pretende obtener son la llave(s) o un algoritmo.

- La llave(s) k.
- Un algoritmo para inferir P_{n+1} de $C_{n+1}=E_k(P_{n+1})$.

2.18. Conclusiones

Uno de los aspectos que hoy en día es de suma importancia es la seguridad informática en todas sus áreas que la conforman.

Dentro de este capítulo pudimos conocer el origen de la criptografía, así también la definiciones y usos más importante de la seguridad, destacando los algoritmos clásicos que en un principio se utilizaban dentro de la evolución de la historia hasta conocer los algoritmos modernos que en la actualidad se utilizan en herramientas de uso común en el web.

El fin principal que se pretende con este capítulo es de podernos empapar de los conceptos básicos de la seguridad, con el fin de poder comprender las herramientas que nos brindan los algoritmos criptográficos, para así poder entender el funcionamiento de la herramienta que integrará a nuestro sitio e-commerce.

Capítulo 3

Servicio Seguro con SSL en Internet

3.1. Historia-SSL Secure Socket Layer

En los comienzos de la utilización del Web se pensó en el uso de la seguridad afortunadamente. La compañia de Netscape Communications comenzó a considerar a un Web seguro; Netscape diseña el protocolo Secure Sockets Layer.

Al comienzo del mes de Noviembre de 1993, con la liberación de Mosaic 1.0 por la National Center for Supercomputing Application (NCSA), se crea Mosaics que fue el primer Web browser. Únicamente ocho meses déspues, Netscape Communications completo el diseño de la versión SSL 1.0 ; cinco meses déspues Nestcape vende el primer producto con soporte para la versión de SSL 2.0 conocido con el nombre de Netscape Navigator.

En este transcurso se incluye la publicación de la versión 1.0 de la Private Communication Technology (PCT) desarrollado por Microsoft ,con muy pocas notables mejorias de la versión SSL 2.0 de Netscape.

Posteriormente se arreglaron las debilidades que presentaba la versión de SSL 2.0 que fueron incorporadas a la nueva versión SSL 3.0. Los próximos eventos representaron un cambio en el estándar de SSL , Netscape Communications desarrollo estas tres primeras versiones de SSL con la significada asistencia de la comunidad del Web. Así de esta manera el desarrollo de SSL fue abierto.

En los comienzos del mes de Mayo de 1996 el desarrollo de SSL llega a ser responsabilidad de los Estándares de la Organización Intenacional-denominada IETF [9].

[9]The Internet Engineerind Task Force

La IETF desarrolló algunos de los estándares de protocolos para internet, incluyendo por ejemplo TCP [10] y IP [11].

Con el fin de evitar la apariencia de la influencia de una compañía en particular, la IETF renombró a SSL con Transport Layer Security (TLS).La versión final de la primera especificación de TLS fue en el año de 1999.

A pesar de los cambios de nombre, TLS no presenta grandes cambios con referencia a la nueva versión de SSL. En realidad, son pocas las diferencias que existen entre la versión de TLS 1.0 y la de SSL 3.0.[13]

En estos momentos el protocolo SSL es soportado en casi todos los browser y servidores Web en el mundo. Pero como podemos nosotros como usuarios saber que estamos utilizando un servicio seguro con SSL.

Bueno tanto Netscape Navigator o Microsoft's Internet Explorer, opera casi transparentemente el protocolo SSL, los usuarios podrán notar que observando el URLse utiliza el prefijo **https:** para un URL SSL-seguro , o podran ver un pequeño icono que representa a un candado, donde cada browser lo despliega (en la parte inferior) cuando se está utilizando SSL.

En algunos navegadores este icono representa a un candado abierto cuando no se esta haciendo uso de un canal seguro y la representación de un candado cerrado cuando se utiliza Secure Socket Layer.

SSL nos proporciona los siguientes servicios de seguridad :

I. Confidencialidad

II. Autenticación e

III. Integridad en los mensajes a los usuarios.

3.1.1. Otras opciones de Seguridad

El protocolo de Secure Socket Layer provee una efectiva seguridad para las transacciones de la Web, pero ésta no es la única alternativa.

La arquitectura de Internet se basa en los protocolos por capas, donde cada capa esta bien definida su función y se conmunica con la capa que la antecede.

[10] Protocolo de Control de Transmisión-Transmision Control Protocol
[11] Protocolo de Internet-Internet Protocol

Cada una de estas diferentes capas del protocolo pueden suportar servicios de seguridad, aunque cada una presenta ciertas ventajas y desventajas.

En el diseño de SSL se crea totalmente una nueva capa de seguridad, así también es posible incluir los servicios de seguridad en la capa de aplicación o el añadirlos directamente en el córazon del protocolo de red.Otra alternativa sería la utilización de un protocolo paralelo.

Se añade una nueva capa actuando como la capa de seguridad SSL insertandola entre la capa de aplicación HTTP y la capa TCP. Para que este nueva capa pueda funcionar ser requieren algunos cambios en el protocolo tanto de arriba y de abajo.

La capa HTTP presenta un comportamiento similar en conexión con la capa SSL, que el que tenía con la ausencia de esta capa.

Mientras que el comportamiento de la capa de TCP con la capa de SSL se ve representado que la capa de SSL es otra aplicación más utilizando el servicio.

Una de las grandes ventajas que presenta SSL es que permite soportar otras aplicaciones además de HTTP como lo son NNTP (net news tranfer protocol) y FTP (file transfer protocol).

En la siguiente tabla se ilustran cada una de ellas : [13]

Arquitectura de Protocolo	Ejemplo	A	B	C	D	E
Capa individual	SSL	*	*			*
Capa de Aplicaciones	S-HTTP	*		*		*
Integrado en el Protocolo	IPSEC	*	*		*	
Protocolo Paralelo	KERBEROS	*			*	

3.1.2. Capa Individual

El diseño de Secure Socket Layer se decidio crear una nueva capa de protocolo de seguridad. En la siguiente figura (Fig.7) se observa una comparación entre el protocolo tcp/ip y la inserción de la nueva capa de SSL.

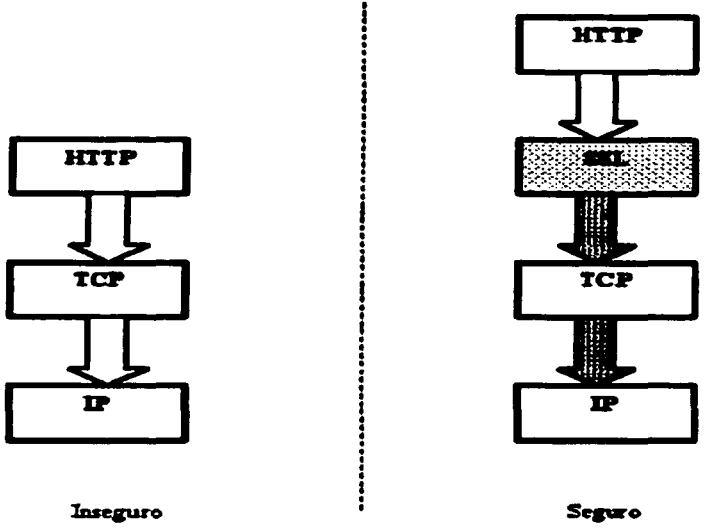


Fig.7

En el fondo se observa la presencia de la capa IP, la cual es responsable de que los mensajes sean routeados a través de la red desde su origen hacia su destino.

La siguiente capa es la TCP construida sobre los servicios de IP con el fin de asegurar que la comunicación sea confiable. Por último en el nivel más alto se encuentra la capa HTTP (Hipertext Transfer Protocol), encargada de entender los detalles de la interacción entre el browser y el servidor Web.

3.1.3. Capa de Aplicaciones

Quizas el diseño de SSL viro hacia una diferente estrategia,donde también es posible añadir un servicio de seguridad directamente sobre un protocolo de aplicación. En el mismo transcurso de tiempo en que Netscape diseño SSL, otro grupo de diseñadores estuvieron trabajando en la idea de un HTTP seguro denotado como s-http.(Fig.8)

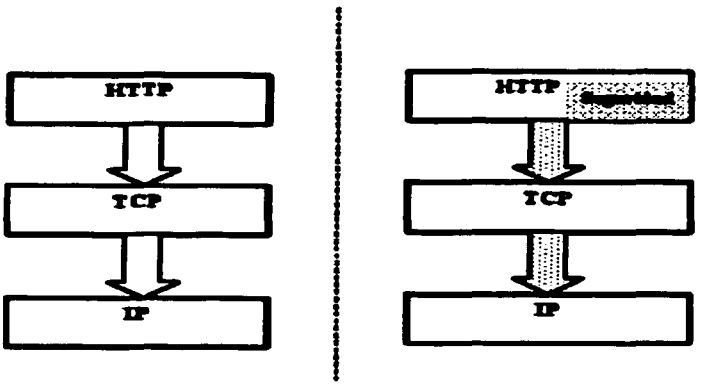


Fig.8

El estándar de HTTP-Seguro ha sido publicado por IETF como un protocolo experimental, pero pocos productos tienen soporte de él.

Una de las grandes desventajas que presenta el añadir seguridad sobre una especifica aplicación es que el servicio de seguridad se encuentra disponible únicamente para dicha aplicación, como en el caso de SSL podía brindar servicio a otras aplicaciones como NNTP, FTP , y el cual HTTP-S no puede.

Y por último el servicio de seguridad que proporciona se liga fuertemente a la aplicación, donde constantemente los protocolos de aplicación cambian así como las necesidades de seguridad.[13]

3.1.4. Integrado en el Protocolo

El protocolo de SSL maneja una capa individual como ya lo hemos visto, mientras que los servicio de seguridad ahora en este caso son añadidos directamente en el córazon del protocolo de red. Nos referimos de IP security(IPSEC) donde los servicios de seguridad llegan a ser completamente parte opcional del IP.

En el siguiente figura (Fig.9) se ilustra la comparación entre el esquema tradicional y el implementado con IPSEC.

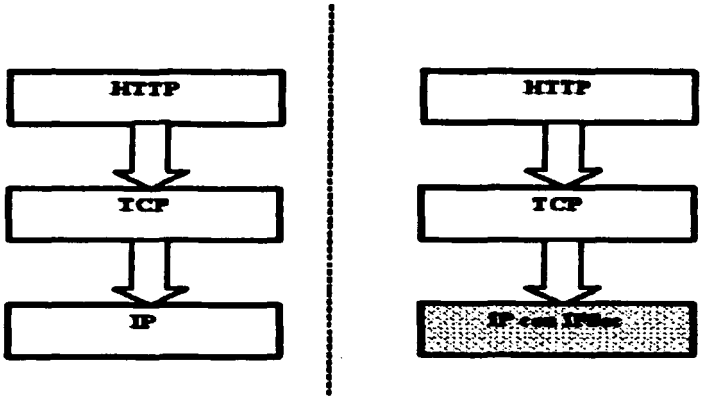


Fig.9

IPSEC tiene algunas de las ventajas que presenta SSL, el ser independiente de la capa de aplicaciones, por lo que la capa de aplicación no debe cambiar del todo para el uso de IPSEC sin embargo IPSEC deberá ser lo suficientemente flexible para poder soportar todas las aplicaciones. Esta complejidad podrá ser un gran factor de retardo en el futuro desarrollo de IPSEC.

Un punto que no es muy favorable para IPSEC es que presenta un gran aislamiento entre la capa de aplicación y el servicio de seguridad, asumiendo que los requerimiento de seguridad se encuentran en función de un sistema en particular y que todas las aplicaciones dentro del sistema requieren el mismo servicio de seguridad.

En cambio SSL podemos decir que también presenta un aislamiento entre la capa de aplicación y el servicio de seguridad pero permite la interacción entre las dos.

Un punto muy importante que se debe de tener muy encuenta es que la aplicación como en el caso de HTTP no necesita cambiar cuando sea agrega el servicio de seguridad , y debe de quedar en manos de la aplicación la decisión de utilizar SSL o no. Dicha interacción hace más fácil para cada aplicación la uilización del servicio de seguridad más apropiado que requiera.[13]

3.1.5. Protocolo Paralelo

El más popular ejemplo de este tipo de protocolo es Kerberos desarrollado por el Instituto de Tecnología de Massachussetts, el objetivo principal de Kerberos es el de proporcionar autenticación y un control de acceso para los recursos en un ambiente distribuido.

El protocolo de Kerberos actua como un conjunto de herramientas en conjunto con otros protocolos que pueden hacer uso de este servicio de seguridad. En el comienzo de desarrollo de los browser's para Web se realizó un esfuerzo para tratar de incorporar kerberos dentro del HTTP, en la siguiente figura (Fig.10) se esquematiza tal arquitectura.

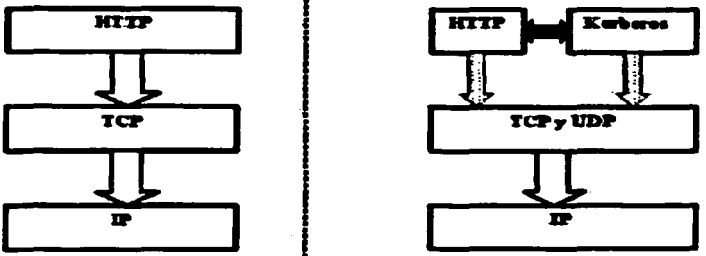


Fig.10

Este trabajo nunca fue completado, en lugar de ello recientemente se ha llevado el esfuerzo para combinar Kerberos con SSL, en tal contexto Kerberos se encarga de proporcionar un intercambio de llave confiable para el mecanismo de SSL.

Por tal motivo se considera a Kerberos como una solución parcial para una solución de seguridad, debido a que no tiene un acceso a la información que actualmente se intercambia en la comunicación entre las dos partes, sin tal acceso Kerberos no puede proporcionar un servicio de cifrado y decifrado.[13]

3.1.6. Limitaciones del Protocolo

Sabemos que SSL se encuentra ampliamente enfocado para proporcionar seguridad en las transacciones Web pero debemos de tener muy encuenta las limitaciones que presenta, las cuales caen generalmente en 3 categorias:

I. Consecuencias del propio diseño de SSL.

II. Debilidades que hereda de las herramientas que utiliza, normalmente de los algoritmos de cifrado y de firmas digitales.

III. Y finalmente del ambiente en el cual SSL fue desarrollado.

Limitaciones del propio diseño

El diseño de SSL requiere de un protocolo de transporte como lo es TCP, este requerimiento es razonable en el mundo de las transacciones del Web debido a que el HTTP por si mismo requiere del TCP. Por tal motivo SSL no puede operar utilizando el protocolo de transporte como lo es UDP.

Otra regla en que SSL falla es soportar el servicio de seguridad de no repudio, podríamos decir que es el equivalente a la firma de datos protegiendo a las partes que lo crean y firman los datos protegiendo a las partes que lo crean y firman los datos para una posterior denegación de los hechos.

Limitaciones heredadas por herramientas

SSL es simplemente un protocolo de comunicación y alguna implementación de SSL debe de confiar en algunos otros componentes estos incluyen a los algoritmos criptográficos.

Estos algoritmos ejecutan actualmente tareas dentro de SSL como el cifrado y decifrado del flujo de la información que viaja sobre el canal de comunicación.Algunos algoritmos criptográficos han sido atacados con éxito aunque en ocasiones se ocultan tales ataques por el miedo de perder presencia en el mercado, como podemos ver esta es una situación importante que debemos de considerar en el momento de la elección del algoritmo que dará soporte a nuestro servidor con SSL.

Limitaciones del Ambiente

Un protocolo de red únicamente puede proporcionar seguridad pra la información que transita por la red, ningun protocolo de red protege los datos antes de que se envían o después de que llegan a su destino.

Esta es la única debilidad conocida pra el Web la cual ha sido explotada con éxito en el actual comercio.

3.2. Funcionamiento de SSL

A continuación explicaremos el caso más simple de SSL el cual consiste en establecer un canal de comunicaciones seguro.

Los puntos que tocaremos serán las opciones que se requieren para la comunicación, también la autenticación en la comunicación entre las partes, separar la autenticación del cifrado y como se llega a una sesión establecida.

3.2.1. Roles de SSL

El protocolo de SSL define dos distintos tipos de roles para la comunicación entre las partes.

Un sistema siempre representa al *cliente* mientras que el otro toma el rol del *servidor*, esta distinción en la arquitectura del cliente-servidor es muy importante ya que SSL requiere de dos sistemas que tomen un rol distintos cada uno de ellos.

Donde el cliente es quien inicializa la comunicación segura y el servidor responde a la petición realizada por el cliente, en el uso más común de SSL quien toma el rol del cliente es el browser del Web mientras que el rol del servidor es adoptado por el sitio Web donde se encuentra alojado el servidor de SSL.

Para el propio SSL es muy importante la distinción entre el cliente y el servidor debido a las acciones que realizan durante la negociación de los parámetros de seguridad que se requieren para establecer el canal de comunicación seguro.

Desde que el cliente comienza la comunicación, este tiene la responsabilidad de proporcionar un conjunto de opciones de SSL que se utilizaran en el intercambio, mientras que el servidor selecciona las opciones propuestas por el cliente que opciones se utilizaran teniendo la última decisión el servidor de la configuración final.

3.2.2. Mensaje de SSL

Cuando se realiza la comunicación entre el cliente y el servidor por medio de SSL se lleva a cabo a través del intercambio de mensajes del SSL, técnicamente SSL define distintos niveles de mensajes.[13]

A continuación mostramos una tabla de todos los mensajes de los distintos niveles, así como su funcionamiento.

Alerta Informa a la contraparte de un posible fallo en la comunicación.

Datos de Aplicación Es la información actual que entre las dos partes intercambian la cual es cifrada, autenticada y verificada por SSL.

Certificado Es un mensaje que contiene la llave pública certificada del cliente.

Petición del Certificado Una petición hecha por el servidor que el cliente proporciona con su llave pública certificada.

Verificación del Certificado Un mensaje del cliente que verifica que el conoce la llave privada correspondiente a la llave pública certificada.

Intercambio del Cifrado Especificado Indica el servicio de seguridad que será utilizado, es decir, el método de cifrado.

Saludo del Cliente Mensaje del cliente indicando el servicio de seguridad deseado por el cliente y que es capaz de soportar.

Intercambio de la llave del Cliente Mensaje del cliente que lleva la llave para la comunicación.

Finalización Indicación de que la negociación es completada y el canal de comunicación seguro ha sido establecido.

Respuesta de Saludo Mensaje de respuesta por parte del servidor que fue iniciado por el cliente.

Saludo del Servidor Mensaje por parte del servidor que indica el servicio de seguridad que será utilizado en la comunicación.

Saludo del Servidor para Finalizar Indicación por parte del Servidor de haber completado todas las peticiones por parte del cliente para establecer la comunicación.

Intercambio de la llave del Servidor Mensaje del servidor que lleva la llave para la comunicación.

3.2.3. Establecer el canal de comunicación cifrado

La función más básica que el cliente y el servidor pueden ejecutar es el establecer un canal de comunicación cifrado.

Tal comunicación queda esquematizada por la siguiente figura:

I. El cliente envía el mensaje **Saludo del Cliente**.

II. El servidor responde con el mensaje **Saludo del Servidor**.

III. El servidor envía la información de su llave pública en el mensaje **Intercambio de llave del Servidor**.

IV. El servidor concluye esta etapa de la negociación con el mensaje **Saludo del Servidor para Finalizar**.

V. El cliente envía información sobre la llave de sesión (cifrada con la llave pública del servidor), con el mensaje **Intercambio de la llave del Cliente**.

VI. El cliente envía un mensaje nombrado **Intercambio del Cifrado Especializado** que podrá ser activado para la comunicación.

VII. El cliente envía el mensaje nombrado **Finalización** que le permitirá al servidor verificar el posible método de activación de cifrado.

VIII. El servidor envía el mensaje **Intercambio de Cifrado Especificado** para activar el método de cifrado que será utilizado mientras la comunicación se de y todo el flujo de información será cifrado por tal método.

IX. El servidor envía el mensaje **Finalización** que le permitirá al cliente verificar la activación del método.

3.3. Descripción de los Mensajes de SSL

3.3.1. Saludo del Cliente

El mensaje de **Saludo del Cliente** comienza con la comunicación del SSL entre las dos partes, es decir, el cliente utiliza este mensaje para preguntarle al servidor el uso del protocolo de SSL.

Este mensaje esta compuesto a su vez por los siguientes componentes:

Versión.- Identifica la versión del protocolo de SSL que será utilizada para la comunicación. **Número Aleatorio.-** Es un número aleatorio de 32 bytes que es utilizado como semilla para cálculos posteriores. **ID de Sesión.-** Identificador de la sesión de SSL. **Juego de Cifrado.-** Especifica los parametros de cifrados para ser utilizados en la comunicación. **Método de Compresión.-** Especifica el método de compresión de datos que será utilizado para la comunicación.

El campo de **Versión** compone al mensaje del cliente para identificar que versiones del protocolo SSL del cliente puede soportar, mientras que el campo del mensaje del Saludo del Servidor determina la versión del protocolo SSL que será utilizado dentro de la comunicación.

El servidor no se encuentra completamente libre de elegir la versión que se utilizará, sin embargo podrá tomar la versión más actual que el cliente pueda soportar.

El campo de **Número Aleatorio** para el mensaje del Saludo del Servidor es esencialmente el mismo que para el mensaje del Saludo del Cliente para el valor de este número pero con l restricción de que el valor es asignado por el servidor.

El campo de **ID de Sesión** contiene un valor que únicamente identifica una comunicación particular del SSL o una sesión del SSL, la principal razón para que explicitamente se identifique una sesión particular de SSL es referirse a esta nuevamente más tarde.

El campo de **Juego de Cifrado** determina el método específico del cifrado así como el tamaño de las llaves que serán utilizadas en la sesión, quien tiene la responsabilidad nuevamente de elegir un método de cifrado es el servidor.

El campo de **Método de Compresión** en general este campo identifica el método de compresión de datos que se utilizará durante la sesión.

3.3.2. Intercambio de la llave del Servidor

Después de que el servidor recibe el mensaje de **Saludo del Cliente** complementa el campo del **Juego del Cifrado** correspondiente al **Saludo dl Servidor.** Mientras que el campo del **Juego del Cifrado** indica el método del cifrado así como el tamaño de la llave, por lo que este mensaje contiene la información de la llave pública.

El formato de la llave depende directamente del algoritmo utilizado. Debemos notar que este mensaje es transmitido sin ser cifrado, así que únicamente la información de la llave pública puede ser.

3.3.3. Saludo del Servidor para finalizar

Este mensaje le dice al cliente que el servidor ha finalizado con la negociación de este mensaje, por si mismo este mensaje no contiene información relevantte pero es importante para el cliente ya que una vez que el cliente recibe este mensaje puede continuar con la siguiente fase para establecer el canal de comunicación.

3.3.4. Intercambio de la llave del Cliente

Cuando el servidor ha finalizado la primera fase de la negociación del canal de comunicación, el cliente responde con este mensaje el cual proporciona la información de su llave hacia el servidor.

En este caso la información de la llave corresponde al esquema de un algoritmo de cifrado simétrico donde ambas partes utilizaran para su sesión.

Además la información del mensaje del cliente es cifrado utilizando la llave pública del servidor con el fin de autenticar al servidor, es decir, que el servidor posee la llave privada correspondiente a la llave pública de tal forma el servidor no podría decifrar el mensaje.

Debemos de tener presente este concepto debido a que podría existir un atacante que interceptara el mensaje por parte de un legitimo servidor y pretender hacerse pasar por el servidor verdadero sin que el cliente lo sospeche.

3.3.5. Intercambio del Cifrado Especificado

Después de que el cliente envía la información de la llave pública con el mensaje de intercambio de la llave se completa la fase preliminar en la negociación del canal de comunicación.

En este punto ambas partes están listas para comenzar a utilizar el servicio de seguridad que anteriormente ha sido negociado.

El mensaje de intercambio del cifrado específico indica que el servicio de seguridad debe ser invocado, esto quiere decir que primero identifica el conjunto de información que define al servicio de seguridad. Esta información incluye un algoritmo específico de cifrado simétrico, así también un mensaje específico de la integridad del algoritmo y una especificación de la llave de este algoritmo.

Para un sistema dado el protocolo de SSL define un estado de escritura y un estado de lectura. El estado de escritura define la información de seguridad para los datos que el sistema envía y en el estado de lectura se define la información de seguridad para los datos que el sistema recibe.

Por lo que ambas partes mantienen un total de 4 diferentes estados : el *estado de activación de escritura, el estado de escritura pendiente, el estado activo de lectura y el estado de lectura pendiente.*

El contenido de los mensaje de intercambio debe tener la siguiente información; una llave, el algoritmo de cifrado, el mensaje de integridad del algoritmo (abreviación de Messange Authentication Code MAC) y los datos de la llave.

Primeramente ellos acuerdan un cifrado y la MAC, entonces podrán intercambiar la información de la llave, únicamente cuando ambas partes se encuentran en un estado pendiente, el sistema podrá comenzar el mensaje de intercambio de cifrado especificado.

3.3.6. Finalización

Inmediatamente después de enviar el mensaje de **Intercambio de Cifrado Especificado** cada sistema envía un mensaje de finalización. Este mensaje de finalización permite a ambos sistemas verificar que la negociación haya sido satisfactoria y que la seguridad no haya sido comprometida.

Dos aspectos importantes el mensaje de finalización es que contribuye en la negociación del juego de cifrado, esto significa que es cifrado y autenticado acorde al juego del cifrado. Si la parte receptora no pudiera decifrar y verificar el mensaje satisfactoriamente sería claramente que se altero el mensaje.

Esto protege nuevamente contra un atacante quien trata de insertar un mensaje ficticio o alterado, si un atacante hiciera esto, tanto el cliente como el servidor realizan el cálculo del valor hash y si lo valores no coinciden puden detectar que el mensaje ha sido comprometido.

La información que conforma el mensaje de finalización es la siguiente:

- Información de la llave.
- Contenido de los mensajes previos intercambiados por los sistemas.
- Un valor especial indicando quien envía, el cliente o el servidor.

3.3.7. Finalizando el Canal de Comunicación Seguro

Quizas como un problema práctico es raramento utilizado, SSL no tiene definido un procedimiento para terminar el canal de comunicación entre las dos partes.

El cerrar explicitamente una sesión protege nuevamente contra un ataque en el que el atacante se encuentra disponible para comprometer la seguridad por medio de una finalización de la comunicación prematura efectuada por él.

3.3.8. Autenticando la Identidad del Servidor

Hasta el momento hemos visto como SSL pude establecer un canal de comunicación seguro entre las dos partes, pero ninguna de las partes puede estar segura de la identidad de la otra.

El uso más común de los cifrados es el poder realizar una transformación de la información para que sea secreta y no pueda ser vista por terceras partes. Existe por tal motivo una vulnerabilidad propia de los algoritmos criptográficos en la que los datos son cifrados pero el atacante pudiera tener todos los datos necesarios para decifrar el mensaje cifrado.

Para evitar este tipo de ataques, SSL incluye mecanismos que le permite a cada una de las partes el autenticar la identidad de la otra. Con este mecanismo, cada parte puede estar segura de que la otra parte es quien dice ser y no un atacante con identidad falsa.

Pero pensemos que es importante autenticar a ambas partes en base al esquema de e-commerce, cuando uno desea realizar una compra haciendo uso del browser del Web por lo que es importante que el sitio Web sea autenticado.

Es claro que no se desearía enviar el número de la tarjeta de crédito a un impostor, por lo que surge la necesidad de realizar la autenticación del servidor.

En la siguiente diagrama se ejemplifica el proceso de autenticación del servidor.

Pasos para autenticar el servidor

I. El cliente envía el mensaje **Saludo del Cliente**.

II. El servidor responde con el mensaje **Saludo del Servidor**.

III. **El servidor envía la información de su llave pública certificada por medio de un mensaje certificado.**

IV. El servidor concluye esta etapa de la negociación con el mensaje **Saludo del Servidor para Finalizar**.

V. El cliente envía información sobre la llave de sesión (cifrada con la llave pública del servidor), con el mensaje **Intercambio de la llave del Cliente**.

VI. El cliente envía un mensaje nombrado **Intercambio del Cifrado Especializado** que podrá ser activado para la comunicación.

VII. El cliente envía el mensaje nombrado **Finalización** que le permitirá al servidor verificar el posible método de activación de cifrado.

VIII. El servidor envía el mensaje **Intercambio de Cifrado Especificado** para activar el método de cifrado que será utilizado mientras la comunicación se de y todo el flujo de información será cifrado por tal método.

IX. El servidor envía el mensaje **Finalización** que le permitirá al cliente verificar la activación del método.

3.3.9. Certificado

Cuando nosotros estamos autenticando estamos identificando una de las partes, es los pasos para autenticar al servidor descritos en la sección anterior el servidor envía un mensaje de **Certificado** en lugar del mensaje de **Intercambio de la llave del Servidor**.

Donde el certificado simplemente contiene una cadena certificada que comienza con la llave pública del servidor certificada y termina con la entidad certificadora.

El proceso de verificación del certificado podría parecer de no mucha trascendencia pero esta representa un punto medular para la seguridad. El cliente debe asegurarse no únicamente de que el certificado es utilizado por una autoridad confiable, si no que el certificado no identifique ambiguamente a la parte con quien desea entablar una comunicación.

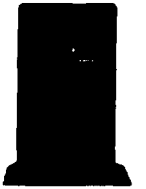
Cabe señalar que dentro del mensaje de Intercambio de llave del cliente ahora el cliente cifra la información utilizando la llave pública del servidor proporcionada en el mensaje de **Certificado** en lugar del mensaje de **Intercambio de llave del Servidor**, en tal caso por lo tanto el servidor se autentica a si mismo.

3.3.10. Autenticando la Identidad del Cliente

Sabemos que el protocolo SSL incluye mecanismos para realizar l autenticación de la identidad del servidor y es natural que también exista un camino para autenticar la identidad del cliente.

A continuación ilustraremos los pasos que se llevan a cabo para realizar la autenticación del cliente.

CLIENTE SERVIDOR



1 Saludo del Cliente →

← Saludo del Servidor 2

← Certificado 3

← Petición del Certificado 4

← Saludo de Servidor Finalizado 5

6 Certificado →

7 Intercambio de la llave del Cliente →

8 Verificación del Certificado →

6 Intercambio del Cifrado Especificado →

7 Finalización →

← Intercambio del Cifrado Especificado 8

← Finalización 9

Veremos que los mensajes que difieren a como se venian manejando son el mensaje de **Petición de Certificado** donde el cliente certifica el mensaje y el mensaje de **Verificación del Certificado**.

Pasos para autenticar la identidad del cliente:

I. El cliente envía el mensaje **Saludo del Cliente**.

II. El servidor responde con el mensaje **Saludo del Servidor**.

III. El servidor envía la información de su llave pública certificada por medio de un mensaje certificado.

IV. **El servidor envía el mensaje de petición de certificado para indicar que desea la autenticación del cliente.**

V. El servidor concluye esta etapa de la negociación con el mensaje **Saludo del Servidor para Finalizar.**

VI. **El cliente envía la llave pública certificada en el mensaje certificado.**

VII. El cliente envía información sobre la llave de sesión (cifrada con la llave pública del servidor), con el mensaje **Intercambio de la llave del Cliente.**

VIII. **El cliente envía un mensaje de verificación de certificado, el cual contiene información firmada acerca de la sesión que utiliza la llave privada del cliente, entonces el servidor utiliza la llave pública certificada del cliente para verificar la identidad del cliente.**

IX. El cliente envía un mensaje nombrado **Intercambio del Cifrado Especializado** que podrá ser activado para la comunicación.

X. El cliente envía el mensaje nombrado **Finalización** que le permitirá al servidor verificar el posible método de activación de cifrado.

XI. El servidor envía el mensaje **Intercambio de Cifrado Especificado** para activar el método de cifrado que será utilizado mientras la comunicación se dé y todo el flujo de información será cifrado por tal método.

XII. El servidor envía el mensaje **Finalización** que le permitirá al cliente verificar la activación del método.

Petición del Certificado

Este mensaje cumple con las especificaciones del servidor en caso de requerir autenticar la identidad del cliente, esto indica que para enviar el mensaje de petición de certificado formará parte de la negociación del saludo.

Sabemos que el servidor enviará la petición del certificado después de enviar su propio mensaje de certificación debido a que las especificaciones de SSL prohibe a un servidor enviar una petición de certificado si este no se ha autenticado por él mismo, esta restricción le asegura al cliente conocer la identidad del servidor antes de revelarle la suya.

El mensaje de petición de certificado esta compuesto por dos campos:

-Tipos de certificado.- Es una lista de los tipos de certificado aceptados por el servidor.
-Nombres distinguido.- Es una lista de nombres distinguidos de la autoridad certificada aceptados por el servidor.

Certificado

Un cliente responde normalmente a la petición del certificado enviando su propio mensaje de certificado después de recibir el mensaje de Saludo del Servidor para finalizar.

El formato del mensaje del certificado del cliente es idéntico al formato del mensaje del certificado del servidor, ambos tienen una cadena certificada comenzando con su propio certificado y terminando con la entidad certificadora. Pero si un cliente no posee un certificado este responde con una alerta informando que no tiene un certificado, entonces el servidor podrá elegir si ignora esta alerta y continua con la comunicación o en su contraparte podrá terminar la sesión en ese punto.

Verificación del Certificado

Simplemente el enviar el mensaje de certificado del cliente no completa el proceso de autenticación de la identidad del cliente, el cliente también deberá proporcionar de que él posee la llave privada correspondiente a la llave pública certificada.

Para tal demostración el cliente utiliza el mensaje de verificación del certificado el cual contiene el valor hash de la información disponible tanto del cliente como del servidor, esta información firmada la comprende la información de la llave y el contenido de todos los mensajes previos que intercambiaron las partes.

3.4. Conclusiones

Este capítulo se centra principalmente en lo que será nuestra herramienta de apoyo para nuestro sitio e-commerce; Secure Scoket Layer se incrusta como una capa individual sobre el protocolo de comunicación entre la capa de HTTP y la capa de TCP logrando de esta manera un canal segurdo donde todo el flujo de información que viaje por este canal será cifrado.

El ambiente en el que se desenvuelve SSL es el cliente-servidor, es importante conocer el funcionamiento de SSL, que parametros envía el cliente al servidor y el servidor al cliente para poder establecer el canal de comunicación.

Después de establecerse el canal de comunicación seguro existen varias cosas atras de ello como el paso de mensaje entre el cliente y el servidor y el conocerlos y entender que sucede es muy importante en el momento de la implementación.

Ahora ya estamos en condiciones de comenzar a realizar nuestra compilación de lo que será nuestro servidor SSL y de las herramientas necesarias para nuestra implementación.

Capítulo 4

Aplicaciones de e-commerce

4.1. Servidor Apache

Más del 60 % de los servidores Web en el mundo utilizan Apache, podemos verlo en la gráficas que muestra la compañia de Netcraft la cual pública periodicamente estadisticas de los servidores más usados, a continuación se muestra una de las gráficas comparativas de los servidores más usados.[18]

4.1.1. Historia de Apache

En los primeros días que se creo el Web, el Centro Nacional para Aplicaciones de Super computadoras (NCSA) creo un servidor Web que llegó a ser el número uno de los servidores al principio de 1995. Sin embargo el primer desarrolo de este servidor al mismo tiempo la gente que estaba utilizando el servidor Web de la NCSA comenzó a intercambiar sus propios parches para el servidor y pronto realizaron un foro para el manejo de los parches.

Por tal motivo surge el primer grupo de Apache, el grupo utilizó el código delservidor Web de NCSA, de esta manera nació un nuevo servidor Web denominado **Apache**. Originalmente derivado del código del servidor Web que en un principio creado por NCSA y manojo de parches, adquiriedo un liderazgo en el mercado.

Las primeras versiones (0.6.2) públicamente distribuidas de Apache fueron liberadas en abril de 1995. La versión 1.0 fue liberada el 1 de Diciembre de 1995. El grupo de apache se ha expandido y operando enteramente vía Internet. Sin embargo, el desarrollo del servidor Apache no es limitado en ningún sentido por el grupo, debido a que cualquiera que tenga los conocimientos de como pude participar en el desarrollo del servidor o en sus módulos este podrá hacerlo.

Quizas el grupo es la autoridad final sobre que esta incluido en la distribución estándar de la que es conocida como la distribución del servidor Web de Apache. Esto permite literalmente a miles de desarrolladores producir nuevas caracteristicas, arreglar bug's, portarlo a nuevas plataformas, y más.

Cuando nuevos códigos se presentan al grupo de Apache, los miembros de Apache investigan los detalles, ejecutan pruebas y hacen un control de calidad de los mismos si estos son satisfechos, el código es integrado en la distribución principal de Apache.[6]

4.1.2. Caracteristicas de Apache

Una caracteristica principal que ofrece apache es que corre virtualmentes sobre todo tipo de plataforma, en su comienzo fue utilizada principalmente sobre Unix pero en casi todas las variantes de Unix, así también corre sobre la plataforma de Windows 2000/NT/9x y algunos otros tipos de sistemas operativos tales como Amiga OS 3.x y OS/2.

Apache ofrece algunos otras caracteristicas incluyendo un buen indexado de directorios; seudónimos de directorios; configuración de los errores de HTTP; ejecución de programas de CGI a través del UID; administración de recursos para los procesos hijos; reescritura del URL; verificación del URL;etc.

Otras caracteristicas importantes que debemos mencionar son las siguiente :

- Soporte para la última versión del protocolo HTTP 1.1
- Una simple configuración basada en un archivo llamado httpd.conf
- Soporte para CGI's
- Soporte para host virtuales
- Soporte para la autenticación de HTTP
- Integra Perl
- Soporte de los script de PHP
- Soporte de Java Servlet Page
- Integra servidor proxy
- Presenta estado del servidor y personalización de logs
- Soporte para Secured Socket Layer SSL.

4.1.3. Licencia de Apache

El software libre tal como Apache, Perl y Linux no comparten el mismo acuerdo sobre el manejo de su licencia y así se ha creado una confusión por asociar estos paquetes en una misma categoria de licencia.

Todos los software libres son pensados para ser libres para todos, pero existen una restricciones legales que la licencia individual de software impone, por ejemplo linux el cual es hecho libre bajo la licencia GNU Public License (GPL), requiere que algun cambio a Linux sea hecho público. Apache, no requiere que los cambios hechos a él sean públicos.

Pensar que Apache como libre, en base a los derechos de software publicados por el grupo de Apache, ni es del dominio público ni es un shareware, también cabe notar que Apache no esta cubierto por la licencia GPL.[14]

4.1.4. Instalación

Antes de comenzar la descripción de donde debemos bajar el código fuente de Apache y notar las versiones actuales que se encuentran libres de bug's o fallas debo hacer incapie que tal instalación es austera y sin ningún aspecto de seguridad alguno, pretendiendo solo introducir en el manejo y forma de instalación del servidor Apache, podría sonar confuso pero podríamos levantar el servidor de Apache sin seguridad alguna, es decir, sin SSL lo cual no nos brindaría nada de seguridad, más adelante veremos como realizar esta instalación.

Antes de descargar el software debemos detenernos a decir que existen dos versiones importantes en la distribución del servidor de Apache la diferencia importante entre estas dos versiones radica en la arquitectura del servidor principalmente, existiendo la versión 1.3x y la versión 2.0.x.

El sitio oficial donde debemos descargar el código fuente del servidor Apache es el siguiente:

http://www.apache.org

Dentro de la página encontrarás distintas secciones donde la que nos interesa es la de *download*, una vez elegida esta opción se nos presentan distintas carpetas de las cuales accederemos a *httpd*.

Una vez ingresado a esta carpeta se nos presentara una lista de archivos fuentes de la siguiente manera:

apache_1.3.27-win32-src.zip apache_1.3.27.tar.Z
apache_1.3.27.tar.gz
httpd-2.0.46.tar.Z
httpd-2.0.46.tar.gz

Podemos observar que el sufijo del nombre de los archivos presentan una extensión que depende de la plataforma y del método de compresión que se uso, nos abocaremos en el uso de la extension **tar.gz** bajo la plataforma Linux Red Hat 8.0.

Proseguimos a descargar el archivo *apache_1.3.27.tar.gz* en su directorio actual, una vez descargado el archivo requeriremos una terminal del sistema para ejecutar las siguientes instrucciones:

```
tar – zxvfapache_1,3,27.tar.gz
cd apache_1.3.27/
./configure
make
su –
make install
```

Dentro el flujo de instrucciones el símbolo de $ corresponde al prompt del sistema, el primer comando que se ejecuta consiste en descomprimir el código fuente podemos observar que la última extensión del archivo es **gz** y **destararear** él código.

El comando **tar** consiste en agrupar un conjunto de carpetas y directorios en un sólo archivo con extensión **tar**. A continuación se especifican las opciones :

z Para descomprimir archivos con extensión gz. **x** Extraer archivos con extensión tar. **v** Desplegar en la terminal. **f** Especificar un archivo.

Una vez realizado esto se generará una carpeta con el mismo nombre del archivo fuente donde se econtrará el código fuente por lo que nos cambiamos al directorio con el comndo *cd*.

Dentro de esta carpeta se encuentra un script llamado **configure** que permite configurar el árbol del código fuente antes de compilar e instalar los binarios.La ejecución del script es como ya se mencionó anteriormente :

./configure [–prefix=apache_installation_dir]

Por default el script realizará la instalación en /usr/local/apache, pero que pasa si deseamos modificar la ubicación de la instalación a través de la opción *–prefix* y especificar una nueva ruta de instalación.

Existen varias opciones que se podran especificar con el script *configure*, pero para el caso de práctica se omiten.

Después de haber configurado el código de Apache, el siguiente paso es compilar e instalar Apache. El siguiente comando a ejecutar es *$make* el cual se encargara de compilar el código fuente.

Y por último se realiza la instalación con el comando *$make install*.Una vez ejecutado este juego de instrucción ya terminamos la instalación del servidor.

Dentro de la estructura que se generó se encuentran los siguientes directorios.

- **include** Contiene todas las cabeceras de archivos de C que son únicamente utilizadas con desarrollos de aplicaciones Web integradas con Apache o hacer uso software de terceras partes con Apache, que pueden requerir estas cabeceras de archivos.
- **lib** Librerias que son requeridas para la ejecución del Servidor Apache.
- **htdocs** Es el documento default utilizado como directorio principal para el servidor Apache.
- **logs** Utilizado para almacenar los *logs* del servidor.
- **cgi-bin** El directorio por default para almacenar los CGI.
- **bin**
  - **ab** Es un programa de apache para realizar pruebas de rendimiento del servidor.
  - **apachectl** Es un script práctico para levantar y parar el servidor (start, restart, stop).
  - **apxs** Esta herramienta permite construir e instalar modulos dinámicos haciendo uso del modulo *mod_so*.
  - **htdigest** Este programa crea y actualiza la información de la autenticación del usuario cuando el mensaje autenticación de firma esta siendo usado.
  - **htpasswd** Este programa es utilizado para crear y actualizar la información de la autenticación del usuario utilizando la autenticación por HTTP.
  - **httpd** Es es servidor del programa Apache
  - **logresolve** Este programa resuleve las direcciones IP del archivo log a los nombre de host.
- **config**
  - **httpd.conf** Archivo de configuración de servidor Apache.
  - **httpd-std.conf** Es una copia del archivo httpd.conf.
  - **mime.types** Define cuales tipos de cabeceras son enviadas al cliente para un determinado archivo.
  - **magic** Este archivo almacena datos para el módulo de mod_mime_magic.

4.1.5. Aspectos de Configuración

En la sección anterior se explicó la manera de como instalar el servidor Apache ahora veremos como configurar el servidor y explicaremos las etiquetas que utiliza.

Por default, Apache lee el archivo de configuración nombrado como **httpd.conf**, por lo general cada distribución viene con un conjunto de archivos de configuración tal directorio es el ya mencionado *conf*.

El archivo de configuración `httpd.conf` contiene dos tipos de información: comentarios y directivas del servidor, donde las lineas que comienzan con el símbolo de # será tratado como una línea de comentario.

4.1.6. Configuración Global

A continuación se explicaran las directivas para un ambiente global del servidor en orden en como aparecen en el archivo de configuración.

ServerRoot

Esta directiva es la primera que aparece en el archivo de configuración, la cual tiene como función especificar el nivel más alto de jerarquía donde se encuentra alojado el servidor Apache. Este directorio no es donde se guardan el contenido de Web y debe de quedar claro si no que únicamente en esta ubicación contiene subdirectorios de todos los archivos relacionados al servidor.

El valor por default que contiene este directiva ServerRoot es colocado el que fue colocado en la directiva de `-prefix` si es que fue utilizada.

PidFile

Esta directiva coloca el PID del proceso, que por default es colocado en el archivo `logs/httpd.pid`, cuyo proceso representa el proceso principal del servidor Apache.

ScoreBoardFile

Esta directiva se encarga de encapsular dentro de una condicional if notificandolo a Apache el estado de ejecución del servidor en caso de haber eleguido el modulo de multiprocesos (MPM) sólo disponible en la versión 2.0.x de Apache.

Timeout, KeepAlive, MaxKeepAliveRequest y KeepAliveTimeout

Timeout coloca el tiempo de descanso del servidor en segundos.

KeepAlive, MaxKeepAliveRequest y KeepAliveTimeout son utilizadas para controlar el estado de vida del servidor.

StartServers

StartServer le dice a Apache que inicialice tres servidores hijos desde su inicio, pudiendo modificar el número de servidores pero el propio Apache es bueno en el incremento de los numeros de procesos hijos que va requiriendo.

MaxClients

El valor por default que contiene esta directiva es 8 de número de clientes que podrá atender el servidor de Apache, pero en caso de utilizar el modo multiproceso podras atender a un máximo de 200 peticiones simultaneamente.

ThreadsPerChild

Define cuantos hilos son creados por proceso hijo.

MaxRequestPerChild

Esta directiva coloca el número de peticiones por proceso hijo que puede atender, el valor por defecto es cero haciendo que un porceso hijo atienda una petición por siempre.

4.1.7. Configuración Principal

La configuración principal del servidor aplica al sitio por default del Web, este sitio es el sitio que es levantado cuando se ejecuta Apache.

Port

La directiva del puerto coloca que puerto TCP por el cual el servidor de Apache escuchara a las conexiones, el valor por default es 80 cuyo valor es el puerto estándar para HTTP. Si se modifica tal valor por ejemplo 8080 únicamente se podrá accesar al servidor utilizando la URL como *http://hostname:8080/* especificando el puerto en el URL.

User y Group

Estas directivas le informan al servidor el user id (UID) y el group id (GID) a utilizar, estas dos directivas son muy importantes en el aspecto de seguridad ya que cuando el proceso padre del servidor lanza un proceso hijo para atender la petición entonces este cambia el UID Y GID del proceso hijo acorde a los valores colocados en las directivas.

Si el proceso hijo corriera como un proceso de tipo root, una potencial vulnerabilidad de seguridad surge dejando la posibilidad a que algun atacante pueda interactuar con un usuario root, por lo que es altamente recomendado elegir una baja prioridad del usuario y así también una baja prioridad de grupo para ejecutar el proceso hijo.

En algunos sistemas unix, el usuario nombrado como **nobody** (UID = 1) y el grupo nombrado **nogroup** (GID = -1) son de baja prioridad. Si se esta pensando en ejecutar el servidor como usuario root no se encontrara disponible el poder cambiar el UID y GID del proceso hijo, debido a que el proceso del usuario root puede cambiar el UID O GID de otros procesos. Por último cabe mencionar que si tu ejecutas el proceso del servidor con el usuario Jorge, entonces todos los procesos hijos tendran los mismo privilegios que el usuario Jorge, de igual forma ocurre con el group ID.

ServerAdmin

Define la dirección de correo que es definido cuanto el servidor genera una página de error.

DocumentRoot

Apache necesita conocer la ruta del directorio raiz donde las páginas Web serán guardadas, este directorio es tipicamente llamado el directorio del documento raiz.

Existen directivas que controlan a los directorios cuyas directivas se encuentran encerrados como sigue:

```
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
```

El alcance de las directivas es limitado al nombre del directorio con algunos subdirectorios, sin embargo se puede hacer uso de directivas que son permitidas en otro contexto de directorio.

UserDir

Esta directiva le dice a Apache que considere el valor de esta directiva como un documento raiz, esto tiene sentido si se tiene multiples usuarios sobre el sistema y se desea permitirle a cada uno de los usuarios tener su propio directorio Web.

DirectoryIndex

Esta directiva especifica que archivos del servidor Apache debe considerar como el índice para el directorio que es solicitado.

La sintaxis de esta directiva es la siguiente:

DocumentIndex archivo1, archivo2, archivo3, ...

Pudiendo especificar multiples archivos de índice, especificandole al servidor de la Web que este debe verificar la existencia de algunos de esos archivos y si alguno de los archivos es encontrado este debe ser regresado a la petición del cliente.

AccessFileName

Define el nombre de acceso de control por directorio, el nombre default es *.htaccess*, la única razon que existe en modificar el nombre de este archivo es el incrementar la seguridad, si deciden modificar este archivo a alguno otro debes esta seguro que cambias la expresion regular "~ht.* "~otro"donde .otro son los primeros caracteres que tu colocaste en la directiva de AccessFileName.

Por ejemplo el archivo contendría <Files ... "~ht» especificandole a Apache la negación de acceso a algun archivo que comience con .ht que es su caso podrían ser .htacces o .htpasswd. Por default se presenta la siguiente configuración.

<Files "^
.ht» Order allow,deny Deny from all </Files>

UseCanonicalName

Cuando esta directiva es colocada en **On**, se le dice a Apache que cree sus propias referencias de los URL's utilizando el formato ServerName:Port.

TypesConfig

Se especifica la ubicación del archivo de configuración *mime.types* que reside en el directorio conf.

DefaultType

Coloca la cabecera de tipo de contenido para algunos archivos cuyo tipo MIME no puede ser determinado por la extensión del archivo.

ErrorLog

La directiva de ErrorLog es muy importante, esta apunta al archivo log encargada de guardar los errores, el valor default es transladado a error_log.

LogLevel

Con esta directiva se especifica la forma de ingresar al sistema que se realizará, el valor por default es warn.

CustomLog

En esta directiva se coloca la ruta para el log de acceso, por default esta utiliza el formato común de log's (common log format CLF), que es definido en la directiva LogFormat.

4.1.8. Arrancando el Servidor Apache

El comando para arrancar el servidor de apache es */usr/local/apache/bin/apachectl start*, si el archivo apachectl se queja acerca de una sintaxis de error se debe corregir los errores que presenta el archivo httpd.conf.

Como podemos verificar que el servidor se encuentra levantado la manera más rápida de hacerlo es con el siguiente comando :

$ ps auxw | grep httpd

Este comando utiliza el comando **ps** para listar todos los procesos corriendo en el sistema cuya información se entuba y se filtra para buscar el proceso de demonio del servidor que en su caso es **httpd**.

Para reiniciar al servidor se ejecuta la siguiente sentencia :

$/usr/local/apache/bin/apachectl **restart**

Y para parar al servidor será con la siguiente instrucción :

$/usr/local/apache/bin/apachectl **stop**

4.1.9. Probar el Servidor

Después de que se ha iniciado el servidor, se accesa a través de un browser utilizando el apropiado host, por ejemplo si ejecutamos el browser localmente donde se encuentra el servidor podemos especificar la siguiente URL *http:/localhost/*.

4.2. Herramientas para el Desarrollo

En la sección anterior se dio una amplia explicación del servidor Apache describiendo minuciosamente sus archivos de configuración y aspectos importantes para su adecuada administración.

Lo que pretendo describir en este apartado, son las demás herramientas de software que se utilizaron para el desarrollo de la tesis. Cabe mencionar que uno de los objetivos que se quiere alcanzar es que el costo del sistema sea lo mínimo por lo que debo recalcar que todo el software que se utilizo es gratuito y bajo la licencia GLP.

Dentro del software que requerimos es un manejador de base de datos que diera soporte a la tienda de comercio electrónico que implementaremos, buscando un manejador que fuera ampliamente conocido en el ambiente y estable sobre la plataforma linux.

El manejador de **Postgres** que contiene toda una infraestructura que un manejador de base de datos debe de tener y que desde sus orígenes fue creado para la plataforma Unix aunque existen esfuerzos para llevarlos a otras plataformas como Windows, otra de sus caracteristicas es que hace uso del stándar SQL y de PL/pgSQL.

En la mayoría de las distribuciones de Linux ya viene el paquete de instalación de Postgres y únicamente con seleccionarlo podras tenerlo instalado en tu sistema Linux, pero en caso de no tenerlo deberas descargalo de http://www.postgresql.org/.

4.2.1. Instalación de Postgresql

Una vez descargado el código fuente de postgres en su caso la última versión utilizada en la tesis fue **postgresql-7.3.2**, donde la serie de comandos que debemos realizar son los siguientes:

$ ./configure

Como primer comando como podemos apreciar es la configuración de la estructura del código fuente a través del script de configuración.

$ gmake

Para comenzar la instalación ejecutas el comando de GNU make(gmake) para realizar la compilación del código fuente.

$ su

Realizas el cambio de usuario mortal al usario root, deben de tener acceso a la cuenta de root si la instalación la realizaras por default de no ser así podras cambiar la ruta de instalación con la opción de **–prefix**.

$ gmake install

Comienzas la instalación de Postgres.

$ adduser postgres

Se agrega un nuevo usuario mortal de nombre **postgres**, menciono que sea un usuario mortal porque es precendible tener un usario con bajos privilegios que será el encargado de levantar el manejador de la base de datos y por medio del cual podras acceder al entorno de desarrolo de Postgres. Cabe mencionar que el ambiente de trabajo natural de Postgres no es muy amigable y es a través de una terminal.

$ mkdir /usr/local/pgsql/data

Creamos una carpeta de nombre **data** la cual será archivos de configuración de postgres y donde se almacenara la base de datos misma.

chown postgres /usr/local/pgsql/data

Modificamos el propietario de dicha carpeta para que sea el usuario que anteriormente creamos en su caso **postgres**.

su - postgres

Una vez realizado esto ya casi acabamos solo queda construir los archivos de configuración de nuestro servidor, con el anterior comando realizamos un cambio de usuario con nombre postgres.

$ /usr/local/pgsql/bin/initdb -D /usr/local/pgsql/data

Este comando es de suma importancia ya que a través de este comando se crean los archivos de configuración del manejador.

$ /usr/local/pgsql/bin/postmaster -D /usr/local/pgsql/data

La ejecuación del comando **postmaster** es quien levanta e inicializa el demonio del manejador de la base de datos especificando el directorio donde se alojaran los datos.

$ /usr/local/pgsql/bin/createdb Prueba

Una vez inicializado el manejador de la base de datos podemos generar una base de datos como lo hacemos con el comando anterior creamos una base de datos de nombre **Prueba**.

$ /usr/local/pgsql/bin/psql

Y por último este comando permite realizar la conexión a la base de datos y acceder a la terminal para interactuar con la base de datos directamente.

4.2.2. Seguridad en Bases de Datos

La seguridad hoy en día es demasiado amplia y podemos encontrarla en cualquier lado que se este haciendo uso de una computadora o un sistema de computo, debido al los alcances de la tesis y el objetivo principal de ella no abarcare demasiado en la seguridad en las base de datos, pero dare un panorama general de ello.

La seguridad en una base de datos se refiere principalmente al **control de acceso, modificación y definición, tanto de los datos como de la estructura de la base de datos** por parte de los distintos usuarios que tengan acceso a la misma.

Sabemos que algunos sistemas operativos nos proporcionan algún nivel de seguridad en el control de acceso a los usuarios, sin embargo este debe radicar principalmente en el DBMS o en la aplicación que maneja la base de datos.

Dentro del sistema manejador de base de datos (DBMS) podemos encontrar un acceso multicapas, como a continuación se explicara (Fig.11) :

- El usuario final debe tener una cuenta valida dentro de la capa del servidor.
- El usuario final debe ser un usario valido dentro de la capa de la base de datos.
- El usuario final deberá tener permisos dentro de la capa de los datos.

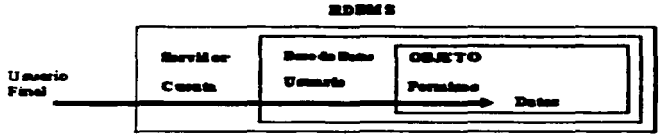


Fig.11

Ahora bien las dos últimas capas se puden traducir en:

- **Seguridad de Objetos**.- Son los permisos de los distintos usuarios que podran hacer uso de las tablas, vistas, procedimientos almacenados, triggers, etc, es decir, todas aquellas operaciones sobre el DDL.
- **Seguridad de operaciones**.- Se manejan los permisos que permiten realizar una modificación como lo son insertar, borrar y actualizar, así también las consultas (operaciones sobre el DML).

A nivel de objetos debemos tener muy presente los siguientes criterios:

- Cada objeto (tabla, vista, procedimiento almacenado) tiene un dueño y que esta propiedad es intransferible.
- El dueño podrá alterar o borrar sus objetos y nadie más, ya sea una tabla, se podrá crear o borrar índices y triggers sobre ella.

- Además podrá otorgar o revocar permisos sobre sus objetos a usuarios, grupos y roles. A su vez podrá determinar si los demás usuarios serán capaces de otorgarselos a otros usuarios lo cual no se recomienda en aspectos de seguridad.

Alguna de las prácticas más recomendadas son que el dueño de los objetos de la base de datos sea un solo usuario, mientras que el DBA es quien realice la generación de los objetos.

El usuario que no es DBA o dueño del objeto, requerirá permisos para realizar alguna de las siguientes acciones sobre objetos ajenos a él.

- Tablas: select, insert, delete, update.
- Vistas: select, insert, delete, update.
- Procedimientos almacenados: execute.

Pero que tipo de permisos no se deben de permitir:

- Todos aquellos permisos que por default quedan en el momento de la creación.
- Índices y triggers.
- El poder de implantar reglas.

Existen comandos importantes que el DBA debera de tomar encuenta dentro de su grupo de trabajo como lo son el comando **grant** que permite otorgar permisos y el comando **revoke** que revoca algun permiso que se había concedido con anterioridad.

4.2.3. PHP

PHP, acrónico de "PHP: Hypertext Preprocessor"es un lenguaje de código abierto interpretado, enfocado para el desarrollo Web y el cual puede ser embebido en páginas HTML.

La mayoría de su sintaxis es similar a C, Java y Perl y es fácil de entenderlo, el objetivo principal de PHP es la creación de páginas dinámicas de una forma rápida y fácil.

El funcionamiento principal de PHP es procesar la información de un formulario, generar páginas con contenidos dinámicos.Dentro de las plataformas que soporta se encuentran todos los sabores de Linux, Microsoft Windos, Mac OS, etc.

Además da soporte a la mayorá de los servidores Web como lo son Apache, IIS de Microsoft, Caudium, OmniHTTPd entre otros.

Da soporte a la programación estructurada y así también a la programación orientada a objetos, quizas una de sus caracteristicas más importantes que destaca el lenguaje es el gran soporte a las base de datos, por mencionar alguna de ellas se encuentran dBase, Informix, Oracle, Sybase, MySQL, PostgreSQL entre otros.

Quizas es muy breve la explicación de este lenguaje pero el objetivo principal es dar un panorama de que es PHP, lo que nos ofrece y que podemos hacer con el, lo más importante que considero es que PHP se pone en competencia con los lenguajes de Microsoft como ASP y de Sun como lo son JSP que tiene el mismo fin, y lo más importante que este lenguaje es de código abierto y no cuesta nada.[15]

4.3. Intalación del Servidor SSL

En las secciones anteriores explicamos las herramientas que se utilizaron en el desarrollo de la presente tesis, realizando la elaboración de un e-commerce del tipo B2C enfocado principalmente en la venta de libros por internet todo esto respaldado por una configuración adecuada del servidor apache y de un canal seguro como lo es SSL.

Dentro de esta sección explicaremos la manera de realizar la instalación adecuada de nuestro servidor apache haciendo la integración del protocolo SSL, así como la especificación del manejador de nuestra base de datos que utilizaremos y de nuestro lenguaje dinámico que haremos uso en su caso PHP.

4.3.1. Apache-SSL-PHP-Postgresql

Bueno empezaremos diciendo que se debe tener mucho cuidado en el código fuente que descarga para la instalación del servidor apache, del módulo de SSL así como de php y postgresql.

Voy a dar por hecho que ya se encuentra instalado el manejador de la base de datos "Postgresql"debido a que ya fue explicado en secciones pasadas, por lo que la intalación que acontinuación se muestra hace referencia a ella.

Lo primero que debemos de hacer es descargar el código fuente de cada una de las aplicación debiendo tener los siguientes códigos fuente :

apache_1.3.27.tar.gz	http://www.apache.org
mod_ssl-2.8.14-1.3.27.tar.gz	http://www.apache.org
openssl-0.9.7b.tar.gz	http://www.openssl.org
php-4.3.2.tar.gz	http://www.php.net

Deberas descargar el código fuente en una carpeta para que posteriormente los descompactemos y sacarlos de la agrupación de paquetes con extensión `tar`.

El código `apache_1.3.27.tar.gz` corresponde al del Servidor de apache.

El código `mod_ssl-2.8.14-1.3.27.tar.gz` corresponde al módulo que se le integrara al Servidor apache y que dará soporte a SSL.

El código `openssl-0.9.7b.tar.gz` corresponde al fuente del protocolo SSL, así como algoritmos de cifrado para proteger el canal de comunicación.

Y por último el código `php-4.3.2.tar.gz` representa el código del lenguaje PHP que dara soporte a nuestro comercio electrónico.

Una vez descargado el código fuente de las respectivas aplicaciones procedemos a descompactarlos y desagrupar los paquetes con las siguientes instrucciones:

```
$ tar -zxvf apache_1.3.27.tar.gz
$ tar -zxvf mod_ssl-2.8.14-1.3.27.tar.gz
$ tar -zxvf openssl-0.9.7b.tar.gz
$ tar -zxvf php-4.3.2.tar.gz
```

A través del comando `tar` realizamos las dos tareas al mismo tiempo descomprimir y desagrupar las carpetas, donde en los argumentos la opción `-z` indica que descomprima el código, con las opciones de `-xvf` desagrupe la estructura del código fuente. Todos estos pasos crean una carpeta con el mismo nombre y versión correspondiente en el directorio actual donde ejecutamos los comandos anteriores.

Dentro de la carpeta actual debemos tener los siguientes directorios que se generaron al descompactar y desagrupar el código fuente.

Una vez realizado esto comenzaremos con la configuración previas a la instalación:

```
cd ./apache_1.3.27
apache_1.3.2$ ./configure -prefix=/opt/Server/apache
```

Nos cambiamos de directorio para estar ubicados en el directorio de apache y ejecutamos el comando de configuración previo a la instalación y yo en mi caso le especifico una ruta a través de la directiva `-prefix` donde deseo que se realice la instalación previamente cree la carpeta de nombre Server ubicada en `/opt` y especifico el nombre de la carpeta donde se alojara toda la instalación.

Recomiendo que tengas terminales distintas para cada una de los códigos fuentes que intalaremos. En otra terminal y ubicados en el directorio donde tenemos nuestros directorios procedemos con la configuración de instalción del código fuente de SSL, se han de preguntar que paso con la configuración del servidorde apache pero volveremos más adelante para su instalación final.

Es importante que sigas esta secuencia de pasos para que la instalación sea la adecuada y llegues a objetivo deseado.

```
$ cd ./openssl-0.9.7b

openssl-0.9.7b$ ./config -prefix = /optServer/ssl
-opensssldir = /opt/Server/dirssl

openssl-0.9.7b$ make

openssl-0.9.7b$ make test

openssl-0.9.7b$ make install
```

Si en la ejecución de alguno de los procedimientos anteriores no tuvimos contratiempo, hemos instalado satisfactoriamente el código fuente de SSL que hará uso el Servidor Apache.

Ahora configuraremos el módulo de SSL para Apache, en una nueva terminal y ubicado dentro de la carpeta de código fuente realizamos las siguientes tareas:

```
$ cd mod_ssl-2.8.14-1.3.27

mod_ssl-2.8.14-1.3.27$ ./configure
-with-apache=../apache_1.3.27 -with-ssl=../openssl-0.9.7 -
enable-shared=ssl
```

Con el comando anterior especificamos que el módulo será agregado en apache y con SSL, especificando las rutas del código fuente de sus rsepectivos directorios. Después de haber ejecutado el comando anterior en la pantalla nos mostrara que debemos reanudar la configuración de apache así como su instalación final.

Regresamos nuevamente a la terminal que en un inicio teníamos donde comenzamos a configurar apache, tenemos que agregar nuevas directivas de configuración.

```
apache_1.3.27$ ./configure -prefix=/opt/Server/apache -
enable-module=most -enable-shared=max -enable-module=ssl

apache_1.3.27$ make

apache_1.3.27$ make certificate

apache_1.3.27$ make install
```

Dentro de los comandos de instalación podemos observar como siempre el comando make que compila el código fuente generando archivos de código objetos para su posterior instalación. El comando más importante y que cabe rescatar es `make certificate` por que a través de él generamos nuestro certificado que será utilizado durante la solicitud a la conexión a nuestro servidor y que es de suma importancia para la autenticación.

Y por último el comando `make install` que realizara la instalación correspondiente en la ubicación especificada en la directiva `-prefix`.

Una vez terminado esto tenemos listo el servidor de Apache con SSL pero aún nos hace falta configurarlo y especificarle que soporte el lenguaje de PHP que acontinuación realizaremos.

```
$ cd ./php-4.3.2
```

```
php-4.3.2$ ./configure -prefix=/opt/Server/php -enable-tracks-var -enable-trans-id -with-pgsql=/usr/local/pgsql/ -with-apxs=/opt/Server/apache/bin/apxs
```

```
php-4.3.2$ make
```

```
php-4.3.2$ make install
```

```
php-4.3.2$ cp php.ini-dist /opt/Server/php/lib/php.ini
```

Una vez realizado todo esto casi ya terminamos sólo nos faltan algunos detalles, en la configuración del servidor de Apache, sólo comento que el último archivo que se copia es importante ya que sera el archivo de configuración de PHP.

Los siguientes pasos consisten en modificar algunas directivas de configuración de apache y el archivo de configuración de php para el buen funcionamiento de nuestro sistema.

No ubicamos en lugar de instalación que especificamos en el momento de la instalación `cd /opt/Server/apache/conf/` para editar el archivo de configuración del servidor Apache `http.conf`.

Donde tenemos que agregar la siguiente línea dentro de la sección de agregar tipos `AddType application/x-httpd-php .php`, una vez agregada guardamos lo cambios y salimos, el fin de la línea es que Apache pueda identificar los archivos con extensión `.php`.

Ahora lo único que nos hace falta configurar es el archivo de configuración de PHP ubicado en `/opt/Server/php/lib/php.ini`, editamos el archivo `php.ini` y buscamos la siguiente línea de configuración `register_globals` que se ecuentra con el valor de `Off` la cual la debemos de enceder con el valor de `On`.

El fin de activar esta variable es para que permita el paso de parametros entre los formularios que se utilizan en el diseño del sitio.

Listo, tenemos nuestro servidor para arrancarlo y ponerlo en servicio, para levantar el servidor es similar a la explicación que dimos en la sección de Apache, nos ubicamos en el directorio de apache dentro de la carpeta de bi- en ejecutando el siguiente comando:

```
apache/bin$ ./apachectl startssl
```

Una vez ejecutado el comando nos pedirá el password que le pusimos en el momentos de generar nuestro certificado.

4.3.2. Construcción del Sitio

Para caso de prueba se construyo un pequeño sitio de comercio electrónico tipo B2C donde se realiza la venta de libros.

Los requerimientos que presentó el diseño del sistema, fueron el poder realizar compras de libro a través de Internet y tener un control administrativo del sistema, es decir, poder dar alta, baja y cambios de los articulos que ofrecemos en este caso los libro, así también de los clientes que tiene acceso a nuestro sistema.

La creación del sistema se llevó a cabo conforme al ciclo de vida de un sistema de software, pasando por las etapas del análisis, diseño, construcción y pruebas del sistema.

El sistema consta de distintas pantallas que permiten el manejo de altas de clientes, bajas de clientes y cambios a los datos del cliente, así también contiene el alta de libros, baja de libros y modificación a los datos de los libros, pero teniendo el acceso únicamente al Administrador del sistema para poder relizar todas estas funciones.

Mientras que para nuestros clientes deberan registrarse antes que nada en el sistema para poder tener acceso a nuestro sistema de compra, donde podran realizar su busqueda de los titulos de libros deseados, llevando el registro en su carrito de compra y poder realizar la transacción del monto a través de su tarjeta de crédito.

Todo esto con el objetivo de brindarle al usuario un sistema seguro y confiable a través de nuestro servidor SSL, teniendo la confiabilidad de que su información personal no será susceptible a cualquier persona que trate de capturar la información que viaja a través de la red.

Dos aspectos importantes de seguridad se encuentran presentes que deben ser cuidados altamente, el primero de ellos es cuando un usuario accesa al sistema proporcionando su login y password, que pasaría si el canal de comunicación viajara en claro , pues simplemente alguien que se encuentre escuchando el canal de comunicación por medio de una herramienta denominada sniffer podría capturar el login y password del cliente y poder accesar al sistema haciendose pasar por el usuario verdadero.

Es muy importante proteger el password del cliente y más adelante se realiza la prueba de escuchar el canal de comunicación teniendo el servidor con SSL y sin SSL mostrando notoriamente como viaja la información a través de la red.

El otro proceso importante es la transacción de compra del producto que se ofrece, cuya transacción se realiza a través del número de la tarjeta de crédito lo cual es sumamente peligroso que caiga en manos de terceros. De igual manera por medio del protocolo SSL nos aseguramos que toda la información que viaje a través de la red sea cifrada por medio de un algoritmo criptográfico.

4.3.3. Sitio e-commerce

Como ya se ha mencionado con anterioridad se realizo la construcción de un pequeño sitio Web tipo B2C con el proposito de modelar un sitio e-commerce.

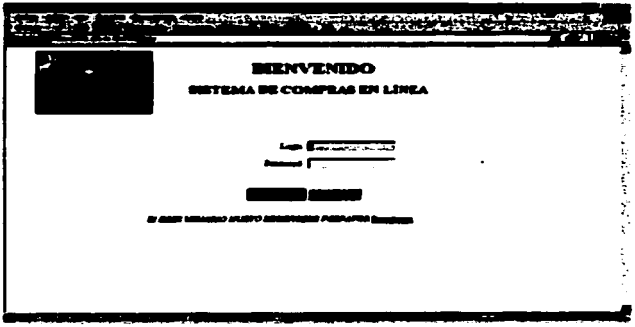
El aspecto administrativo del sistema es básico para el mantenimiento del mismo, permitiendo tener un control sobre la información de nuestros clientes así como de los productos que ofrecemos.

En las secciones anteriores hemos tratado el aspecto más importante que se deben de considerar en la planeación y diseño de sistemas de comercio electrónico que es la seguridad. Ahora quisiera dar un panorama general del funcionamiento del sistema y las partes que lo conforman.

Quisiera explicar algunas de las ventanas principales que conforman al sistema comenzando por la ventana principal o de inicio, hago un parentesis para recordar que el sistema es para Web por lo que todas las interfaces que se generaron fueron elaboradas con HTML,PHP y Java Script, por lo que para el buen funcionamientto del sistema se necesita una versión mínima del navegador así como el tipo del navegador que utilicemos.

Este comentario lo hago debido a que Java Script presenta problemas de compatibilidad en sus versiones y en el navegador que se este utilizando por lo que recomiendo la utilización de Internet Explores 5.0 o superior para el buen funcionamiento del sistema.

Después de este gran parentesis comienzo explicando cada una de las interfaces que conforman al sistema y su funcionamiento.

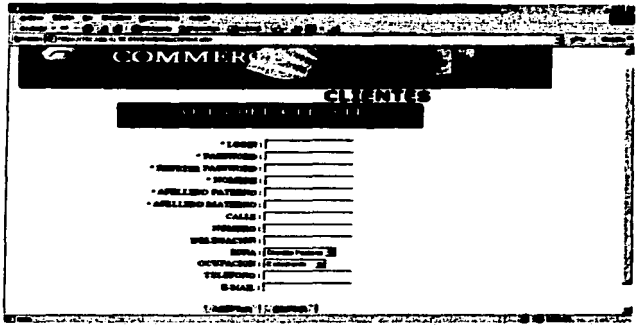


Pantalla de inicio. **Fig.12**

Como podemos ver se utilizó un método tradicional de seguridad para el control de acceso a nuestro sistema como es el ya bien conocido **login y password**, por el cual tenemos el control de nuestros clientes a nuestro sistema de compras.

Como podemos apreciar el sistema da soporte a que si se tratase de un nuevo cliente, se registre ante el sistema para que nos proporcione los datos necesarios para ser dado de alta y le sea asignado un **login y password** para su acceso.(Fig.12)

La siguiente interfaz es darse de alta por primera vez ante el sistema podemos decir que se trata de un cliente nuevo.(Fig.13)



*Pantalla para darse de alta.***Fig.13**

En esta interfaz se presenta un formulario al cliente nuevo para que proporcione la información adecuada ante el sistema y quede registrado y lo más importante asignarle un login y password para su posterior acceso al sistema de ventas de libros en línea.

Después de llenar los valores obligatorios el cliente estará dado de alta al sistema y podrá accesar a él con su **login y password** asignados.

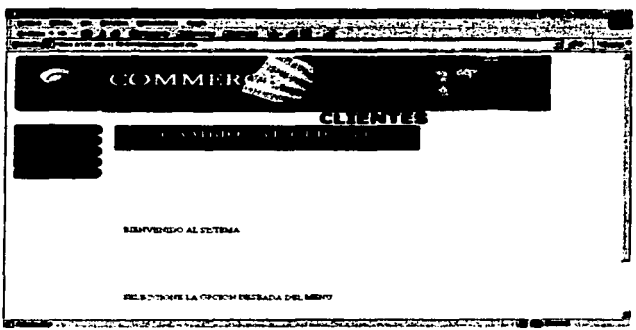
Como he venido mencionando y siendo algo reiterativo el sistema se conforma de la parte administrativa y la parte que el cliente tiene acceso al sistema por lo que el acceso es restringido para el cliente normal, a diferencia de los privilegios que tiene el administrador de este sistema.

Que quiero decir con todo esto, el administrador del sistema tiene privilegios especiales que una persona común o un cliente no pueden tener, un administrador tiene los privilegios de poder realizar bajas, cambios y altas de los artículos que se ponen a la venta.

También el administrador tiene los privilegios de modificar los datos de un cliente que ya se encuentre registrado en el sistema o dar de baja en el propio sistema, todos estos privilegios y caracteristicas peculiares que he descrito no las puede tener un usuario normal o común porque donde quedaría la integridad propia de nuestro sistema si permitimos que un cliente normal pudierá dar debaja a otro sin la autorización pertinente.

Por lo cual existe un usuario nombrado **root** que es nuestro administrador de nuestro sistema y pose el mayor de los privilegios para el funcionamiento del sistema.

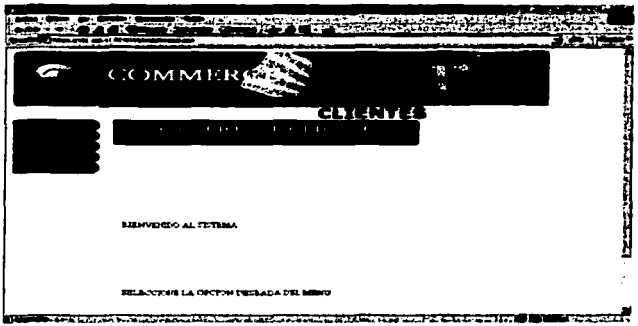
Una vez ingresado al sistema con un **login y password** autenticado adecuadamente, dependiendo de si fue un cliente normal o si fue el administrador variaran las operaciones en las funciones del menú presentado.



*Pantalla principal para el administrador.***Fig.14**

Lo importante que hay que apreciar en esta interfaz es el menú de la parte izquiera que presenta distintas opciones para realizar nuestras tareas, dentro de las cuales se le presentan al administrador; la sección de clientes, la sección del producto de venta, la sección de compras y la sección de consultas.(Fig.14)

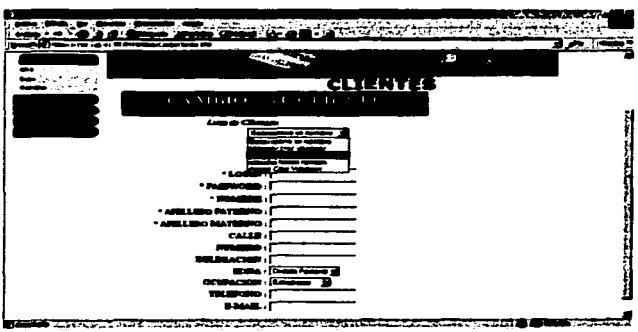
Más adelante se explicará el funcionamiento de cada una de estas secciones, el punto principal es ahora distinguir entre las distintas opciones que tiene el administrador.



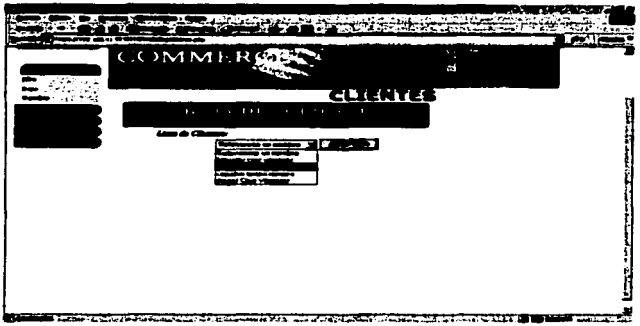
*Pantalla Principal para el cliente.***Fig.15**

Como vemos a diferencia de la interfaz del administrador, el menú para un cliente es la sección de compra que es el fin principal para que el cliente ingresa, realizar compras de nuestros libros y la sección de consulta para que el usuario pueda consultar las compras que ha realizado.(Fig.15)

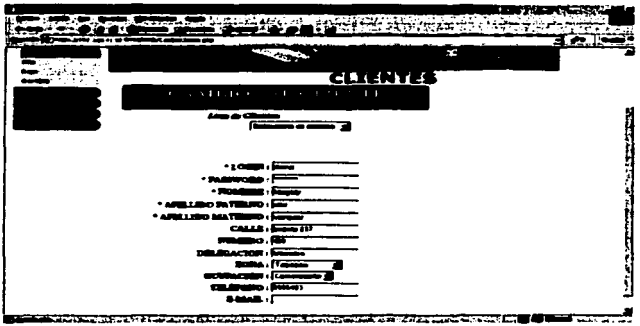
Esta interfaz es el punto de partida para las operaciones que pueden realizar nuestros clientes.(Fig.16,17 y 18)



*Pantalla para Alta de un cliente.***Fig.16**

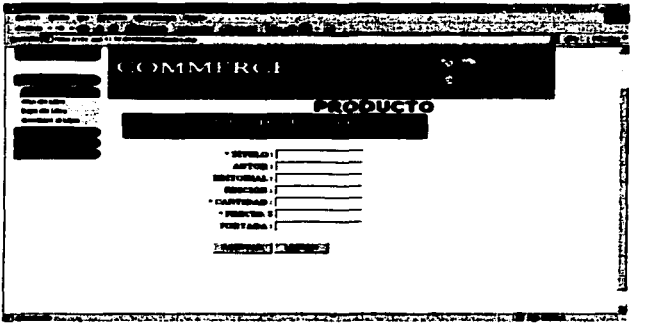


*Pantalla para Baja de un cliente.***Fig.17**

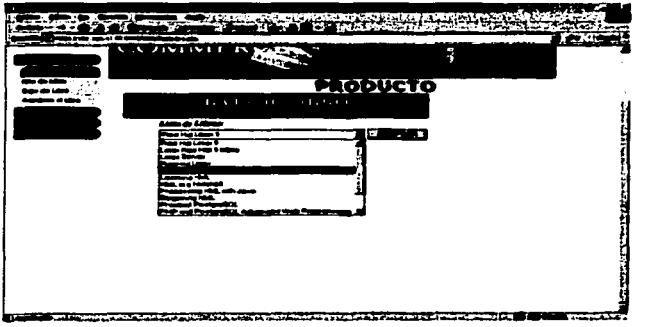


*Pantalla para Cambios de un cliente.***Fig.18**

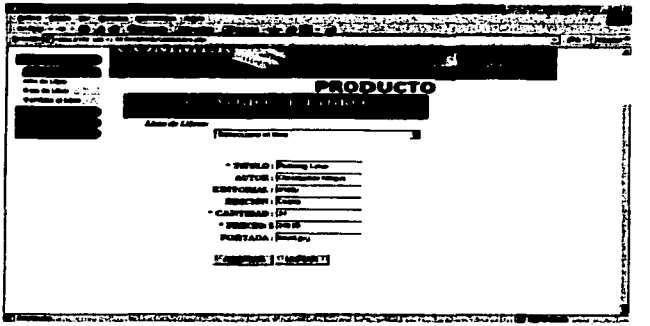
Por medio de estas tres interfaces el administrador del sistema podrá tener el control y actualización de la información de los clientes pudiento actulizar la información del cliente o dar de baja un cliente o más bien dicho un ex-cliente.(Fig.19,20 y 21)



*Pantalla para el alta de un libro.***Fig.19**

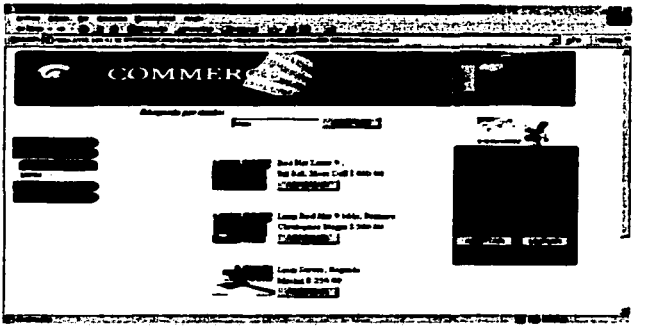


*Pantalla para la baja de un libro.***Fig.20**

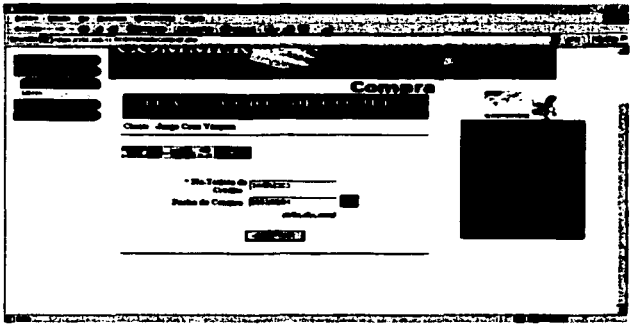


*Pantalla para el cambio de un libro.***Fig.21**

El producto principal que se le brinda a nuestros clientes son nuestros libros, por lo que requerimos del registro de los ejemplares con que contamos, como el monto y control de las piezas que contamos de cada uno. Por tal motivo el fin de estas tres interfaces que anteriormente ilustramos es mantener un control adecuado de nuestro producto y actualizaciones de precios, cantidad o baja de algun libro que ya no se vende en nuestra tienda electrónica.



*Primer pantalla de compra.***Fig.22**



Segunda pantalla de compra. **Fig.23**

Las interfaces anteriores son las más usadas para el cliente ya que en ella podrá realizar busquedas de los títulos de libros que desee comprar, una vez encontrado el título del libro podrá ir agregandolos en su carrito de compra que se encuentra en la parte derecha de la pantalla.

El carrito de compra siempre se encuentra presente durante el proceso de compra para que el cliente tenga presente lo que llevá elegido, podemos notar que dentro del área del carrito de compra se encuentran dos botones, uno de aceptación con el cual se indica que quiere continuar con el proceso de compra y quiere realizar el pago de los libros que eligio y el otro boton es para vaciar el contenido del carrito.(Fig.22 y 23)

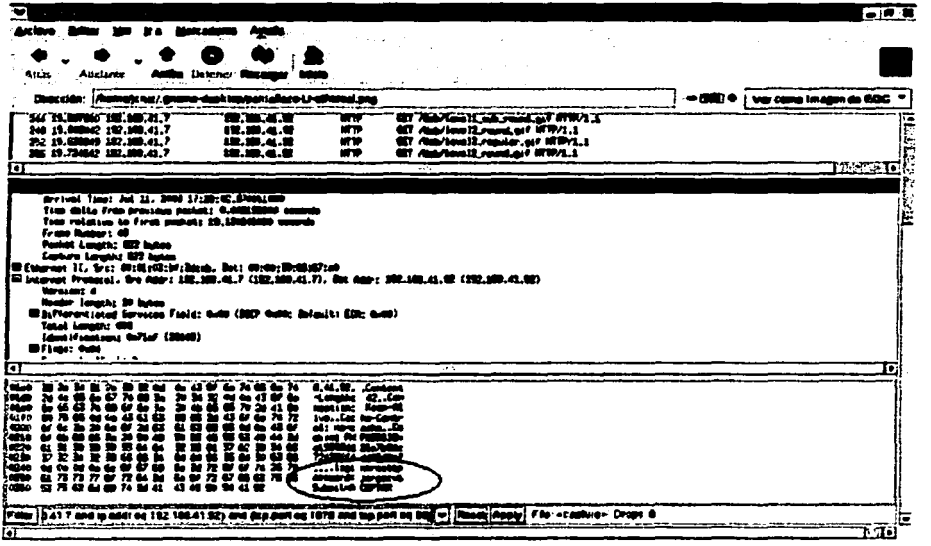
4.3.4. Pruebas al sistema

Como venía mencionando, un intruso podría colocar un sniffer para captar todo el flujo de información entre el emisor y receptor por lo que realizamos la prueba a nuestro sistema e-commerce colocando un sniffer con ausencia del protocolo SSL y cuando tiene el protocolo SSL nuestro servidor.

Con esta prueba podemos darnos cuenta de las vulnerabilidades que se pueden presentar si no implantamos un esquema de seguridad en nuestro servidor.

La primer imagen que mostraremos es la que captura el momento en que un cliente se conecta a nuestro sistema y accesa a él a través de su **login** y **password** por medio del sniffer Ethereal vemos como el login y password de nuestro cliente viaja en claro, lo cual significa una gran vulnerabilidad para el sistema que un intruso pueda obtener dicha información.(Fig.24)

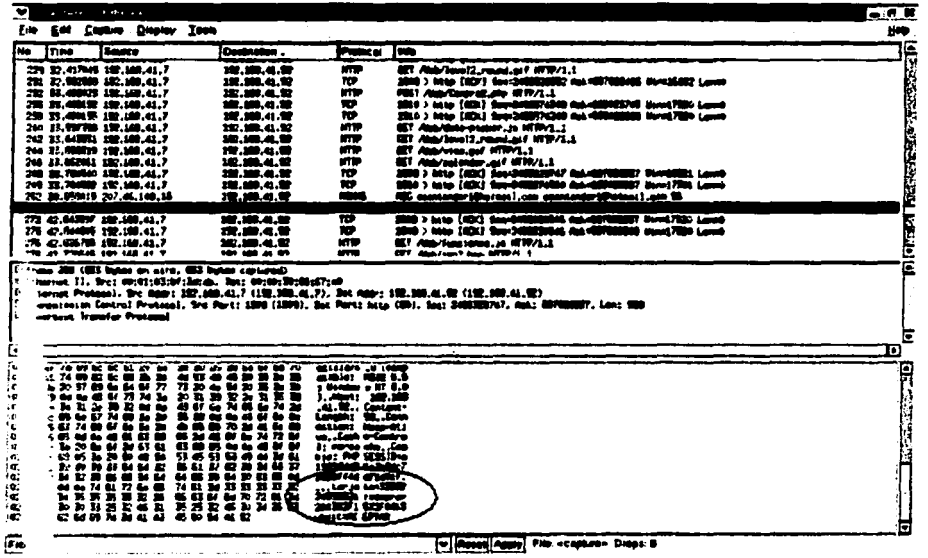
Cabe aclarar que esta pruebas son con el servidor normal sin SSL.



Captura del login y password. **Fig.24**

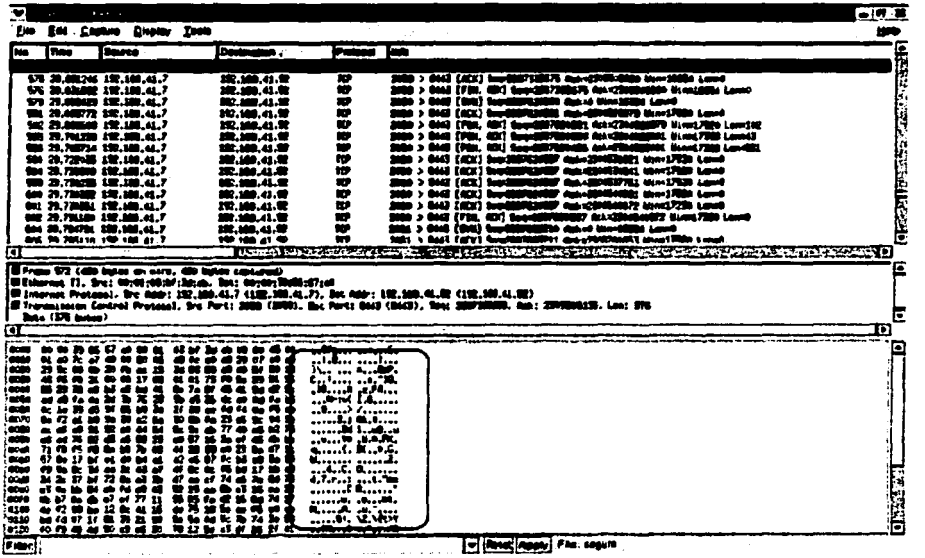
Otro proceso importante y de vital importancia que debemos proteger es el número de la tarjeta de crédito de nuestros clientes, el cual en nuestra siguiente imagen mostramos como viaja también en claro cuando nuestro servidor no se encuentra implementado con SSL.(Fig.25)

El campo que contiene el numero de tarjeta tiene el nombre de **tarjeta** y se encuentra encerrado en un circulo para identificarlo.



*Captura del número de la Tarjeta de crédito.***Fig.25**

Por último hicimos las mismas pruebas pero con el servidor con SSL y podemos apreciar como la información que viajaba sin ser cifrada ahora no es entendible a simple vista debido a que toda la información viaja cifrada.(Fig.26)



Captura de información con el servidor SSL. **Fig.26**

Con esto estamos garantizando la confiabilidad de nuestro sistema y que terceras personas no puedan obtener información relevante a nuestros clientes.

Conclusiones

- Pudimos conocer los distintos esquemas que se encuentran en el mercados electrónico como lo son sus tres principales vertientes B2B, B2C y B2G, pero principalmente a que grupos de mercados se encuentran dirigidos.
- Llevamos a la práctica un módelo de comercio electrónico como lo fue nuestro pequeño sitio B2C de bajo costo y que brinda un servicio seguro. Este bajo costo del sistema se logro utilizando herramienta de software libre.
- Debio de haber cambiado la forma de pensar y ver las cosas después de ver la fragilidad y la vulnerabilidad que pueden presentar nuestros sistemas si no se aplican buenas políticas de seguridad así como esquemas de seguridad que protegan nuestra información contra terceras personas que no tienen la autorización de acceso a ella.
- Estar consientes que el canal de comunicación que se da en el Web es lo bastante inseguro para que se puedan cometer fraudes millonarios, acceso a cuentas no permitidas, robo de información, perdida de informacion, y así podría seguir numerando infidad de peligros que nos podemos enfrentar en la red debido a que no se tiene un adecuado conocimiento de los mecanismos de seguridad que uno debe implementar.
- Conocimos los mecanismos de seguridad que existen, los algoritmos criptográficos, conocer las vulnerabiliadades que se presente en las herramientas que utilizamos para protegernos, revisando constantemente los sitios web de las organizaciones que distribuyen el código fuente y actualizando constantemente nuestro servidor, con ello evitaremos darle más herramientas al criptoanálista.

- Se desarrollo un sitema B2C, cuanta con la posibilidades de seguir creciendo en el aspecto de poder ofrecer diversos productos a nuestros clientes, no únicamente libros si no otro tipo de articulos.
- Los alcances que se pretendieron en un inicio de la tesis se cumplieron con la finalización del sistema pero cabe señalar que por parte del aspecto de seguridad puden ser añadidos otros esquemas de seguridad a nuestro sitio e-commerce haciendolo más robusto, como podría ser un esquema de control de acceso por medio de la herramienta **Kerberos** la cual se agregaría a nuestro manejador de base de datos postgresql.
- Si se pretende realizar un sistema a mayor escala donde se involucre a un equipo de trabajo se deberán tomar las medidas necesaria que en seguridad se refiere en el control y administración al manejo de la base de datos.
- Que cualquier persona interesada en colocar su propio sitio web tome las referencias aqui planteadas como base para su propio diseño e implementación de su pripio sitio e-commerce.
- Por útlimo debemos estar consiente que no existe un sistema 100 % seguro y debemos de tenerlo muy presente. La forma de pensar y realizar nuestras actividades cotidianas están cambiando día con día y con la ayuda del avance de las nuevas tecnologías modificará nuestra manera de pensar y realizar nuestra vida.

Bibliografía

[1] Abhijit Chaudhury;Jean-Pierre Kullboer. E-BUSINESS AND E-COMMERCE INFRAESTRUCTURE.

[2] Ewald Geschwinde;Hans-Juergen Schoenig;Hans-Jurgen Schonig. PHP AND POSTGRESQL ADVANCED WEB PROGRAMMING.

[3] Fúster;Dolores de la Guía Martínez;Luis Hdez Encinas. TECNICAS CRIPTOGRAFICAS DE PROTECCION DE DATOS. Segunda Edición. Alfaomega.

[4] Jesus Castagnetto;Harish Rawat;Sascha Schuman;Chris Scollo and Deepak Valiath. PHP PROGRAMMING. Wrox Press.

[5] John C. Worsley;Joshua D. Drake. PRACTICAL POSTGRESQL.

[6] Kabir Mohammed J. APACHE SERVER 2 BIBLE.

[7] Kenneth C. Laudon;Carol G. Traver;Carol Guercio Traver. E-COMMERCE: BUSINESS,TECHNOLOGY,SOCIETY.

[8] Menezes A.J. HANDBOOK OF APPLIED CRYPTOGRAPHY. CRC Press.

[9] Pfleeger Ch.P. SECURITY IN COMPUTING. Segunda Edición.

[10] Richard Stones;Neil Matthew. BEGINNING DATABASES WITH POSTGRESQL.

[11] Schneier B. APPLIED CRYPTOGRAPHY PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C. Segunda Edición.

[12] Simson Garfinkel;Gene Spafford. SEGURIDAD PRACTICA EN UNIX E INTERNET. O'relly.

[13] Stephen Thomas.SSL AND TLS ESSENTIALS.

[14] http://www.apache.org/

[15] http://www.php.net/

[16] http://www.openssl.org/

[17] http://www.postgresql.org/

[18] http://news.netcraft.com/archives/