11
2 ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

SISTEMAS DE SEGURIDAD EN COMPUTO

SEMINARIO DE INVESTIGACION INFORMATICA

QUE PARA OBTENER EL TITULO DE :

LICENCIADO EN INFORMATICA

P R E S E N T A :

LETICIA LÓPEZ NAVA

ASESOR DEL SEMINARIO:
ING. SANTIAGO SUAREZ CASTAÑON

MEXICO, D. F. 1998

FCA

TESIS CON

Agradecimientos

(no creo que exista algo con que agradecerles, pero ...)

Papá y Mamá

"Nunca te orgullezcas de tus frutos. Sólo eres dueño del esfuerzo que pusiste en su cultivo; de lo que se logra, nada más eres espectador... Su vuelo depende de tu fuerza, pero también del viento y, ¿por qué no decirlo?, del destino que camina detrás de ellos."

Ermilo Abreu Gómez

Independientemente de como lo sienta,
lo mucho o poco que hasta ahora haya logrado
ante sus ojos,
más que mío es suyo.

Leticia

Abue:

Creo que la deuda que tengo contigo es bastante más grande que la de 1 peso por cada 10 de calificación (mejor así lo dejamos).

Francisco y Alicia:

Por mis hijas

Hermanos:

Jennifer, Mónica, Alejandro, Tanna, Tanno y Carolina. Gracias por soportame (aunque no lo hagan).

Doctora Castillo:

Gracias, sin ese cambio al principio de la carrera, quizá no lo hubiera logrado.

Amigos:

Danny, Gabby, Toño, Carmen, Vianey, Ana Lilia. Hubiera sido difícil llegar sin ustedes. (están mencionados en orden de aparición).

A Santiago por la paciencia y los conocimientos para el desarrollo de este trabajo.

Y también a todos los que no mencione.

Indice

Introducción

A partir de la segunda mitad de este siglo que finaliza, nos hemos vuelto más dependientes de las computadoras porque no sólo las utilizamos para realizar nuestro trabajo, sino también para nuestras laborares cotidianas, incluyendo las compras y toda clase de entretenimiento.

En el tiempo en que vivimos, la información es una de las cosas que más ha cobrado valor, y nuestra computadora (así como otros medios relacionados con ésta) es la encargada de almacenar grandes cantidades de información, que bien puede ser laboral, personal o financiera y si no tenemos el cuidado suficiente esta información puede llegar a manos que pueden hacer un mal uso de ésta, llegando a perjudicamos no sólo en nuestro patrimonio sino hasta en nuestra vida privada. Este riesgo se agrava si la máquina se comunica con otras vía red.

Consciente de los riesgos que corren día a día nuestros sistemas de cómputo, mi trabajo de investigación, Seguridad en Sistemas de Cómputo, está enfocado a en primer lugar, a describir las principales amenazas que pueden sufrir nuestras computadoras, así como algunas leyes de las que podemos hacer uso cuando una amenaza se convierte en delito; segundo, dar algunas recomendaciones para evitar amenazas en contra de nuestra información; el tercer punto en el que se centra éste trabajo es el describir algunas formas de encriptación que pueden ayudar a nuestros datos para mantenerse seguros mientras están en transferencia y por último hago la descripción de como se realizan las comunicaciones de forma segura a través de la red de comunicaciones más grande.

La seguridad en los sistemas de cómputo es un campo muy extenso y variado, pero el que nos hagamos responsables de nuestro sistema hace que los riesgos que nos podrían llegar a afectar se vean disminuidos.

CAPITULO I

Amenazas a los Sistemas de Cómputo

En nuestros días la información es considerada como un bien, debido al enorme valor que representa tanto para las empresas, para los gobiernos y los particulares. La cantidad de información producida, almacenada, manejada y transmitida día a día por medio de computadoras es inimaginable y además representa el liquido vital de cualquier área de cualquier empresa que no podrían operar sin los sistemas de cómputo; otra buena razón por lo que las computadoras son una herramienta indispensable es el ahorro significativo en cuanto a recursos humanos y materiales y muchos otros beneficios que esta tecnología con lleva.

Como suele ocurrir con todo lo que representa algo de valor es la información también es susceptible de sufrir algún daño, que implícitamente afecta a su fuente de origen (organización), y si esta información tiene varias fuentes o varios receptores, entonces los afectados son muchos. Y a diferencia de los bienes físicos no puede ser custodiada por su naturaleza intangible.

En los inicios de los sistemas de cómputo, se crearon medidas para asegurar que la información (y el equipo mismo) estuvieran a salvo de cualquier deterioro. El constante avance de la tecnología ha dejado esas medidas preventivas obsoletas. Pero el incremento de redes interconectadas, los equipos de cómputo portátiles y la existencia de gente que tiene a su alcance esta herramienta y que esta más preparada en cómputo; ha hecho que el perpetrar los sistemas de cómputo con finalidad de lucro o daño se haya vuelto común; especialmente para personas que están muy familiarizadas con el ambiente de cómputo y que saben que existen muchas debilidades en los sistemas.

Muchas organizaciones han sido objeto de daños por parte de algún tipo de atacante. Pero muy pocas lo han dado a conocer, en gran parte por la publicidad dañina que les generaría, especialmente si son organizaciones que se dedican a manejar dinero. Y de las pocas empresas que han puesto demanda por haber sido atacadas en su patrimonio, a nivel jurídico poco o nada se ha podido hacer, porque son aún no existe ningún esquema que abarque por completo esta área que todavía es bastante nueva y está en evolución constante.

En este capítulo trataremos primero hacer un esbozo de las características que se deben tener para que un sistema de cómputo sea seguro (que es nuestro objetivo), después veremos lo que puede afectar nuestra seguridad, quienes pueden afectar la seguridad y una breve descripción de la protección jurídica con que se cuenta en estos momentos a nivel internacional.

El área de cómputo abarca muchos conceptos (hardware, software, redes, personal, datos y comunicaciones, etc.; los cuales generalizaremos bajo el nombre de sistema de cómputo). En algunas ocasiones se hablará de manera general y en otras se hablara de conceptos en especifico.

1.1 Objetivos de la Seguridad de los Sistemas de Cómputo

Entre todas las características que debe tener un sistema para que se considere seguro destacan: la confidencialidad, la integridad y la disponibilidad tanto de la información como de los elementos de cómputo relacionados con esta. A continuación detallo cada una de las características.

1.1.1 Confidencialidad

La confidencialidad o privacidad se refiere a que los bienes (información, equipo) de un sistema sean accesibles sólo por personas autorizadas. El tipo de acceso puede ser: conocimiento de la existencia del bien, acceso de lectura o impresión.

1.1.2 Integridad

Significa que los bienes pueden ser modificados sólo por personas autorizadas, en formas autorizadas. Bajo este contexto, la modificación incluye: escritura, modificación, cambio de estado, borrado y creación. Existen tres aspectos de integridad: las acciones autorizadas, separación y protección de recursos y la detección y corrección de errores.

1.1.3 Disponibilidad

La disponibilidad es un tanto compleja, ya que se aplica tanto a los datos como a los servicios, de manera que sólo personal autorizado pueda tener acceso a ellos en todo momento.

Algunas expectativas de la disponibilidad son:

- Presencia del objeto o del servicio con disponibilidad de uso
- Capacidad para cubrir los servicios requeridos
- Tiempo de espera límite

- Tiempo adecuado de servicio/sin servicio

Los objetivos de la disponibilidad son:

- Respuesta en tiempo
- Tolerancia a fallas
- Alojamiento (en memoria) justo
- Disponibilidad de uso
- Control de concurrencia.

Hasta hace poco la disponibilidad se tomaba poco en cuenta y se hacia más énfasis a las áreas de confidencialidad e integridad; provocando varias deficiencias en la otorgación de servicio y acceso a los datos, retrasando o perjudicando la actividad de muchas personas.

1.2. Grietas en la Seguridad

La seguridad continuamente se ve expuesta a pérdida o daño total o parcial del sistema de cómputo; algunos ejemplos de esto pueden ser las revelaciones no autorizadas de información, modificación de información o negativa de servicio de cómputo.

Para el propósito de esta tesis, se tomaron en cuenta tres fases para lograr el infringir un sistema de cómputo.

Las fases son: Detección de Vulnerabilidad, Posibles Amenazas y Ataques Consumados. Podemos decir que, las vulnerabilidades son debilidades del sistema de seguridad que puede ser aprovechadas para causar pérdida o daños. Las amenazas son circunstancias (debilidades) por las que se puede causar pérdida o daño. Un ataque es una amenaza cumplida.

1.2.1 Detección de vulnerabilidad

Como ya mencionamos antes una vulnerabilidad es una debilidad del sistema que no ha sido detectado por los creadores-administradores del sistema y que tarde o temprano puede afectar la funcionalidad de este y en el peor de los casos su seguridad.

Los principales puntos de vulnerabilidad son el hardware, software, datos y comunicaciones:

Hardware: es lo que incluye la computadora básica, las terminales, impresoras, módem, discos, cintas y algunos elementos internos de una computadora como CD, discos duros etc.

Software: existen dos categorías de software; sistema operativo y programas de aplicación.

Datos: son el líquido vital de muchas empresas, tanto el hardware como el software en muchas casos puede ser remplazable no así los datos. Los datos son generados de todo lo que la organización hace. Cuando la gente roba datos, están robando un bien, tal como si robaran dinero o equipo.

Comunicaciones: El conectar una computadora a una red, inevitablemente incrementa la vulnerabilidad de la información almacenada.

1.2.2 Posibles Amenazas

Una vez detectadas las principales vulnerabilidades, se hace un análisis para ver de que forma pueden ser dañadas.

Destrucción de hardware

Generalmente son empleados molestos o terroristas, los que representan esta amenaza. También pueden entrar los accidentes.

Robo de Hardware

Los componentes de hardware son objetivos atractivos para los ladrones especialmente porque pueden ser revendidos fácilmente. Este tipo de robo no sólo deshabilita el equipo sino que también puede redundar en pérdida de datos críticos o en robo de mecanismos de almacenamiento.

Robo de Software

Puede ser robado en como parte de un robo de computadora o por si sólo. Los ladrones pueden tomar discos o cintas que contenien copias de software comercial, o peor aún pueden robar copias de software desarrollado por la organización. El software es una propiedad intelectual, si la competencia llega a tener un sistema completo y funcionando, no tendrán que invertir su tiempo y dinero desarrollando y si pueden lucrar con este. Existen otros tipo de robos de software, como en el caso que los empleados copian software comercial del trabajo para llevarlo a casa.

Sabotaje por computadora

La gente que obtiene control sobre los sistemas que controlan la información de la defensa, la transferencia de trillones de dólares diarios por medio de redes de transferencia de fondos, procedimientos médicos, navegación de aerolíneas, etc. puede causar mucho daño, tanto a los sistemas como a las personas que dependen de ellos.

Algunos tipos de sabotaje resultan obvios, pero hay otros que no lo son tanto, como es el caso de los virus, que accidentalmente aparecen, y por lo general su origen es desconocido, por lo que siempre se tomará como accidentales los daños que puedan causar.

Robo de bienes.

Billones de dólares son robados cada año, por medio de fondos electrónicos de transferencia, almacén, cuentas de pensión y otros varios tipos de fraude.

Robo de resultados.

Algunos crímenes simplemente se relacionan recogiendo datos valiosos en un disco, cinta o papel y llevárselos.

Uso no autorizado.

Existen varios tipos de uso no autorizado, el primero se refiere a el uso de una computadora por gente que no esta autorizada a hacerlo. El segundo es el uso de la computadora por empleados para actividades fuera de las labores de la oficina, cada vez que una computadora es encendida y un empleado gasta su tiempo en cuestiones fuera de labores de oficina, le cuesta dinero a la empresa.

Accidentes

Este tipo de amenaza puede afectar tanto al hardware, al software y a la información. Los accidentes pueden ser naturales (fuego, terremoto, inundación, .., etc.) que por lo regular son poco frecuentes, no así los accidentes humanos que son los más comunes y van desde derramar líquido sobre algún equipo hasta borrar información valiosa.

1.2.3 Ataques Consumados

Se refiere a cuando el sistema tiene pérdidas o daños. La clasificación de los ataques se hizo en base a el objetivo de este trabajo, Seguridad en los Sistemas de cómputo:

- Rompimiento de la seguridad física
  Cuando hablamos de seguridad física, nos referimos a la protección de los edificios donde están alojados los sistemas de cómputo, equipo de cómputo y medios de almacenamiento

- Rompimiento de la seguridad personal
  Se refiere a la protección de la gente que trabaja en cualquier organización y por ende la protección del equipo y datos de esta gente.

- Rompimiento de comunicaciones y datos
  Protección de software y datos , especialmente los que se transmiten de computadora a computadora.

- Rompimiento en operaciones de seguridad
  Protección de la seguridad de los procedimientos utilizados para prevenir y detectar baches en la seguridad y desarrollo de los métodos de prevención y detección.

1.2.3.1 Rompimiento de la seguridad física

La seguridad física se relaciona con protección física de una computadora, equipo de cómputo, medios de computación y todo lo relacionado con cuestiones físicas que van de desastres naturales, accidentes de varios tipos y ataques intencionales. La forma en como puede ser rota dicha seguridad son:

- Basureros
  Mucha información importante (resultados, investigaciones, balances) que debería ser destruida, por que no toda puede ser almacenada, es tirada a la basura, como resultado mucha gente consciente de esto va a los depósitos de basura para encontrarse con información que les puede representar muchos beneficios. Las instalaciones de cómputo son buenos lugares para los basureros, que muchas veces encuentran la información que necesitan para penetrar en los sistemas. En las oficinas y en la basura, los crackers pueden encontrar discos usados, impresiones, apuntes de muchos tipos y papel reusable con datos importantes. Mucha de esta información puede aparecer después en públicaciones de todo tipo.

Otra forma de basurear, que muchas veces no es tomada en cuenta, es cuando en el sistema existen archivos que han sido borrados lógicamente pero no físicamente, por lo que pueden ser recuperados por medio del comando undelete (en el caso de MS-DOS).

- Intercepción de redes

  Existen varios métodos por los que se pueden interceptar redes y comunicaciones. Los cables de teléfonos y redes no están tan protegidas como debieran, que pueden ser dañadas físicamente y poner un dispositivo en los cables para obtener información de la que esta fluyendo a través de estos cables.

  Los criminales cuentan con métodos para escuchar las comunicaciones. Por lo que es importante dentro de la seguridad en las comunicaciones mantener un sistema seguro de cableado para protegerlas de intercepción y vandalismo.

- Emanaciones eléctricas

  Las emanaciones eléctricas de una computadora es un riesgo del que hay que estar consciente. El equipo de cómputo como cualquier otro equipo eléctrico emite impulsos electromagnéticos. Cada vez que se golpea una tecla, un impulso es enviado al área circundante. Por los que estas emanaciones electromagnéticas pueden ser monitoreadas, interceptadas o decodificadas. A pesar de que puede sonar muy sofisticado es muy común.

- Negación de servicio

  Existen dos tipos de ataques en esta categoría. Algunos se refieren a sabotaje electrónico que tiene que ver con la destrucción o deshabilitamento del equipo o de los datos. Apagando el equipo o enviando mensajes para detener la actividad es un ejemplo del primer ataque.

  Otro tipo de ataque es el llamado inundación, o mejor conocido como gusanos, que poco a poco van saturando la máquina impidiendo trabajar a los procesos o crear nuevos.

  La negación de servicio no tiene una técnica compleja de ataque. Aveces ocurre por accidente.

1.2.3.2 Rompimiento de la Seguridad Personal

Aunque muchos de los ataques que se describen pueden caer en este apartado (ya que las personas son quienes los cometen y los evitan) se describe especialmente los siguientes:

- Máscaras

  Ocurre cuando una persona utiliza la identidad de otra para obtener acceso a otra computadora. Esto puede ser en forma remota o local. Existen formas tanto físicas como electrónicas de realizar máscaras. Se habla de ataque físico de máscara cuando una persona se introduce a un centro de cómputo haciéndose pasar por otra. Las máscaras electrónicas se dan cuando se utiliza id, password o identificación personal para accesar una computadora o datos importantes. Los passwords no autorizados utilizan son los más comunes los más efectivos. Si un extraño roba o obtiene por otra forma un password, no hay forma de decidir si la persona que esta accesando es la legítima o algún intruso. Desafortunadamente los passwords son fáciles de adivinar, debido a que muchas personas utilizan el nombre de seres queridos y relativamente cercanos así como el nombre de mascotas o fechas significativas.

  Para entender como funciona las máscaras, se necesita saber algunos cosas básicas de como obtener acceso a sistemas compartidos a través del proceso de identificación y autenticación.

  La identificación es la forma en que el sistema conoce al usuario y la autenticación es la forma de probar que el usuario es quien dice que ser.

- Ingeniería Social

  Es el nombre que se le da a los ataques que usan a otras personas para obtener información para robar datos o introducirse a un sistemas.

- Hostigamiento

  Es cuando se envían correos electrónicos amenazadores, especialmente vía Internet.

- Piratería de Software

  Más adelante detallaremos los términos que utilizamos en esta sección y nos sirven para designar estos crímenes. Mucha gente no

toma los Derechos de Autor seriamente. La gente sigue haciendo copias de juegos a amigos o llevándose software de la oficina para la casa. Las investigaciones de este tipo de robo es muy costoso. Los empleados necesitan ser educados acerca de la legalidad, ética y las políticas de la compañía relacionadas con la piratería de software.

1.2.3.3 Rompimiento de Comunicaciones y Datos

En esta categoría se incluye a los ataques que pueden ser objeto los datos, software ya sea ataque a información almacenada o información que en determinado momento esta siendo transferida vía red, Internet.

- Ataque a los Datos

  Como mencionamos antes, se debe mantener la Integridad, Confidencialidad y Disponibilidad de los datos. El robo, la copia no autorizada de datos confidenciales es un ataque obvio que afecta las características de seguridad de los datos antes mencionada.

- Copia no Autorizada de Datos

  La piratería de software, podría parecer otro ejemplo de copia no autorizada de datos. Los métodos para detectar y prevenir tal crimen se aplican de la misma manera que si fuera para la defensa, banca o personal. Dos términos se escucharan en el contexto de los ataques de datos son: inferencia y fuga de información.

  A través de la inferencia, un usuario legítimamente puede accesar pequeñas partes de información, pero al relacionar esas pequeñas partes puede deducir información secreta. Con fuga de información, un usuario puede accesar un flujo de información por medio de una ruta que no le es permitida. Detectar y prevenir este tipo de ataques requiere de políticas coordinadas entre diferentes categorías de seguridad en cómputo. En términos de seguridad personal, la educación de los usuarios es vital. En términos de operación, el registro automatizados y auditorías de software también juegan un papel importante.

- Tráfico de Análisis

  En algunas ocasiones el ataque a los datos no es tan obvio, aun la información común, es decir que no es clasificada como importante, puede ser importante para los espías industriales o extraños. Este tipo de ataque no necesita de herramientas o medios sofisticados, basta con tener un poco de información y relacionarlo con determinados hechos para llegar a una conclusión.

- Canales de Conversión
  Es una forma de fuga de información disfrazada, puede ser que un reporte común y corriente sea convertido de tal manera que contenga un password.

- Ataque de Software
  Puede ser que el software sea modificado para producir información equivocada, que simplemente no funcione o envíe replicas a un lugar no autorizado.

- Puertas Falsas
  Es una trampa insertada en los programas que le permite a los desarrolladores traspasar toda la seguridad en el sistema. Permitiendo hacer modificaciones al programa. Puede ser que estas trampas se hayan hecho a propósito o que hayan sido producto de algún error por parte de los programadores y descubiertos después por crackers. La detección de trampas se un problema de seguridad operativa.

- Secuestro de Sesión (Session Hijacking)
  Puede darse el caso cuando se deja una sesión abierta y un intruso modifica la información; también se da el caso cuando un sistema no se desconectan inmediatamente después de que una sesión es terminada, y en su lugar permite reaccesar el programa interrumpido por poco tiempo, un cracker que tiene un buen conocimiento de operaciones de telefonía y telecomunicaciones pueden tomar ventaja de este hecho reconectando una sesión terminada.

  Incluso el atacante puede conectar otra terminal a una línea entre la terminal autorizada y la computadora. El criminal espera hasta que la terminal autorizada esta en línea pero no en uso, y se conecta, el servidor piensa que todavía esta conectada al usuario autorizado y el criminal accesa los mismos archivos que haría el usuario autorizado.

- Túneles
  Los túneles se caracterizan por utilizar un método de transferencia de datos para acarrear datos de un método a otro. Los túneles son un método legítimo para pasar información entre redes que son incompatibles, pero es ilegítimo cuando se acarrea información no autorizada en paquetes de datos legítimos.

- Ataques Periódicos
  Es una técnica compleja para tener acceso no autorizado a software

o datos. Cuando dos procesos están compitiendo por recursos, un cracker que tenga buenos conocimientos de Unix, puede hacer que el sistema apunte hacia el programa del cracker y al real. Los sistemas que procesan varias cosas al mismo tiempo, un programador hábil puede penetrar el sistema dándole más privilegios a su trabajo para no tener que formar parte de una cola esperando servicio por parte de los recursos del sistema, en el mejor de los casos pero también puede ocasionar que los programas se estrellen o varios programas se mezclen.

- Caballos de Troya

  Un caballo de Troya es un método para inserta instrucciones en un programa de tal forma que el programa realice funciones no autorizadas, mientras aparentemente trabaja normalmente. Los caballos de Troya son una técnica común para plantar otros problemas en computadoras, incluyendo virus, gusanos, bombas lógicas, y ataque de Salami. Los caballos de Troya son un método común para cometer fraudes computarizados que son difíciles de detectar.

- Virus y Gusanos

  Tanto los virus como los gusanos son confundidos constantemente, ambos pueden ser introducidos en un sistema vía caballos de Troya. En términos de computación un virus es un programa que modifica otros programas de tal forma que puedan replicar el virus; un gusano es un programa que actúa sólo, existe independientemente de otros programas. Para correr no necesita de otros programas, simplemente se replica en una computadora y trata de infectar otra que están conectadas a la red.

  Algunos virus y gusanos son no destructivos, mientras que otros son extremadamente dañinos. Muchos virus de PC, causan que la máquina se estrelle o se pierda información. Un virus es hecho para causar daño, tales virus son designados para estrellar el sistema entero en una fecha determinada o después de varias autoreplicas. El impacto potencial de un virus es limitado sólo por la imaginación del criminal que lo escribió. Algunos crackers ven a los virus como intentos intelectuales.

  La mejor manera de prevenir virus y gusanos de invadir un sistema es:

  1. Ser precavido cuando se introducen datos o software a la computadora.
  2. Usar un rastreador de virus.
  3. Hacer respaldos frecuentemente.

- Salamis

  Este tipo de ataque funciona en datos financieros. Esta técnica consiste en quitar pequeñas cantidades de información de una gran cantidad. La información robado es quitada en pequeñas porciones (de aquí su nombre). Generalmente, la cantidad robada es tan pequeña que la víctima del fraude del Salami nunca lo llega a notar.

  Un ataque teórico financiero de Salami, se relaciona con el redondeo de balances, y llevándose la cantidad sobrante a otra cuenta. A veces estos robos son descubiertos por una auditoría bancaria.

- Bombas Lógicas

  Una bomba lógica típica le dice a la computadora ejecutar un conjunto de instrucciones en un momento determinado bajo especificas condiciones para causar daño. Las bombas no necesariamente se basan en el tiempo para explotar, lo pueden hacer después de que es ejecutado un programa en particular. Este ataque generalmente es perpetrado por gente interna que se le pide salir de la compañía.

1.2.3.4 Rompimiento en Operaciones de Seguridad

Son las encaminadas a incorporar procedimientos para prevenir y detectar todo tipo de ataques en sistemas o al personal.

- Falsa Entrada de Datos (data diddling)

  Se refiere a la modificación de datos antes o después de haber sido introducidos en la computadora.

- Obtener la Dirección del Servidor Adivinando

  Es un tipo de máscara, que sólo puede ser prevenida por operaciones de seguridad fuertes. Determinados programas de UNIX dan acceso basado en dirección IP, esencialmente se autentifica al sistema corriendo el programa en lugar del usuario individual. El atacante falsifica la dirección como si lo enviara de una red interna, en donde los sistemas confían uno en otro. Y gracias a que el atacante aparenta ser parte de la red nunca se le pregunta su identificador o password.

- Adivinación de password

  Las personas que se dedican a introducirse en otros sistemas, pueden monitorear todo tipo de trafico en redes. Para conocer un password se coloca un programa que recolecta los 128 primeros bytes de cada conexión de red que esta en proceso de monitoreo. Cuando los passwords son encriptados resulta más difícil el conocer el password.

- Rastreo (scan)

  Con el rastreador, un programa conocido como un demonio, procesa una serie de información en flujo que cambia en forma secuencial, que bien puede ser una lista de teléfonos o passwords. Probando con cada una de ellas para ver cuales obtienen una respuesta positiva.

- Exceso de privilegios

  Si un atacante accesa una cuenta, puede dañar la información de esa cuenta, pero no puede pasar de los límites de esa cuenta para afectar la información de otros, pero si ese usuario tiene exceso de privilegios; es decir privilegios que no necesita para el tipo de actividades que desarrolla, el intruso puede explotar esa debilidad del sistema para causar una serie de daños en cadena.

1.3. Objetivos de ataque

Los objetivos se ataque pueden ser diversos, pero existe una clasificación de acuerdo al tipo de actividad, por lo que tenemos que existen :

Ataques militares o de Inteligencia

Afortunadamente en México, este tipo de casos no es muy común, más bien es menos que común, pero en otras naciones es un problema de seguridad nacional muy fuerte, debido a que las computadoras almacenan y transmiten información que va desde la posición de satélites hasta planes de artefactos de guerra.

Ataques a negocios

Las empresas son constantemente objetivos de ataque tanto de sus competidores como de curiosos o por empleados resentidos.

Ataques financieros

En estos días, el dinero se maneja vía bits, números en una pantalla de computadora o tinta de alguna impresora. Los cheques son depositan electrónicamente de igual manera las cuentas (de la luz, el servicio de cable, etc.) .Los fraudes más grandes son electrónicos.

Ataques Terroristas

Muchos grupos subversivos han encontrado en las computadoras un buen medio para causar daños.

Bromas

Muchos crímenes son cometidos más como un reto intelectual que como beneficio, algunos se inician incluso como bromas .

1.4. Leyes Aplicables

El sistema legal se ha adaptado en la medida a sus posibilidades a la tecnología de la computación, reutilizando algunas viejas formas de protección legal (Derechos de Autor y Patentes) y creando leyes donde las existentes no se pueden adecuar. Las leyes y la seguridad de cómputo se relacionan en varias formas.

Las leyes regulan el aplicar los derechos de individuos para mantener asuntos personales en forma privada, también se regula el uso, desarrollo y propiedad de programas de datos. Patentes, Derechos de Autor y Secreto de Mercado son mecanismos legales que protegen los derechos de desarrolladores y propietarios de datos y programas. Un aspecto muy importante en la seguridad del cómputo es controlar el acceso a los programas y los datos; tales mecanismos son soportados por la ley. Las leyes también tienen acciones que pueden ser tomadas para proteger los secretos, integridad y disponibilidad de la información y servicios de cómputo.

La ley no siempre provee de un control adecuado, ni en los asuntos de cómputo ni en otros. En lo referente a computación, la ley se desenvuelve lentamente, debido a que las computadoras comparadas con otros bienes son totalmente nuevas.

Gracias a esto su lugar dentro de la ley no esta muy bien establecido. Conforme los casos se van presentando la ley se va definiendo. Pero aún la ley no alcanza a cubrir todos los actos impropios que se cometen a través de las computadoras. Además tanto los jueces, abogados y la policía no entienden la forma como opera y funciona una computadora, así que es muy difícil que determinen como la computación se relaciona con otras partes de la ley.

Las leyes referentes a la seguridad de sistemas de cómputo afectan a programadores, diseñadores, usuarios y a quienes mantienen los sistemas de cómputo, así como bases de datos. Estas leyes proveen de protección pero también regulan el comportamiento de la gente que usa las computadoras. Además , los profesionales de cómputo están entre los mejor calificados para abogar por cambios en las viejas leyes y la creación de nuevas. Pero antes de recomendar un cambio, se debería tratar de entender la ley actual, y a su vez los abogados entender un poco el funcionamiento de esta tecnología para poder establecer bases sólidas.

Para la protección de código y datos se tiene a los Derechos de Autor, Patentes y Secretos de Mercadeo. Es indispensable entender las diferencias fundamentales entre el tipo de protección que estas tres leyes proveen y como se deben aplicar. Es mejor prevenir la violación del sistema que procesarlo el delito una vez ocurrido. De cualquier forma si un control falla, una acción legal debe ser tomada. Un aspecto muy importante es que la ley, también tiene que cuidar de el derecho de la privacidad de datos y de los individuos.

1.4.1 Derechos de Autor y Los Trabajos de Cómputo

Desde 1976 la ley de Derechos de Autor ha incluido una definición explícita del software de cómputo. De cualquier forma los Derechos de Autor puede que no sea la mejor manera de proteger los trabajos de cómputo.

Para verlo mejor hay que considerar el algoritmo detrás del programa. El algoritmo es una idea, las líneas del programa son la expresión de la idea. Por lo que, la protección se encamina hacia las líneas del programa no al diseño, copiar el código intacto esta prohibido pero reimplementar el algoritmo esta permitido.

Un segundo problema con los derechos del Derechos de Autor es que el trabajo debe ser públicado. Un programa puede ser públicado distribuyendo copias del código. Si el objeto fuente no es distribuido, este no ha sido públicado.

La protección de Derechos de Autor no se limita el tipo de uso del trabajo, sólo la distribución de las copias. El área de protección de Derechos de Autor a los trabajos de cómputo, todavía es nuevo y puede ser objeto de muchas interpretaciones en la juzgado. Por lo que muchos aspectos de trabajos de cómputo son objeto de protección de Derechos de Autor.

Derechos de Autor Fueron diseñados para proteger la expresión de las ideas. El Derechos de Copia, hace énfasis en que una forma particular de expresar una idea pertenece al autor. Da el derecho exclusivo de hacer copias de la expresión y vendérselas al publico. Esto es, sólo el autor puede vender copias de su idea.

Sólo el que creó la idea puede obtener los derechos de Derechos de Autor; si una idea no tiene un autor determinado, entonces los derechos de Derechos de Autor no pueden ser otorgados.

La idea que pretende obtener los Derechos de Autor debe estar en un medio tangible, o sea que, una historia o una obra de arte deben estar escritas, impresas, grabadas, o almacenada en algún medio magnético o estar de alguna forma concreta. Otra característica importante de los derechos de Derechos de Autor es el promover la distribución del trabajo.

1.4.2 Patentes

Las Patentes protegen los inventos, fueron creadas para aplicarse a resultados de ciencia, tecnología e ingeniería, mientras que Derechos de Autor fue para proteger el arte, la literatura, y trabajos escolares. Una Patente puede ser válida para algo que es una novedad o es único, así que sólo puede haber una Patente por cada invento. Un objeto patentado también debe ser no obvio. Si un invento resulta obvio para un persona que conoce del área de invención, entonces no se puede otorgar la Patente.

Es poco frecuente porque este tipo de protección no es la apropiada para los algoritmos, que es lo que los desarrolladores desean proteger. Y por el tiempo y el dinero que se tienen que invertir para obtener y mantener la Patente, resulta difícil para los generadores de software a pequeña escala el obtener esta protección.

1.4.3 Secreto de Mercado

A diferencia de la Patente o el Derechos de Autor, la información tiene valor si se mantiene en secreto. Los Secreto de Mercados es la información que da una compañía sobre sus competidores. La característica principal es que siempre debe mantenerse en secreto. Si alguien obtiene un Secreto de Mercado de manera inapropiada y tiene beneficios con ello, el dueño puede demandar para recobrar los beneficios ganados por el otro, así como daños y perjuicios y los costos legales.

Este tipo de ley se aplica muy bien a cuestiones de software de cómputo. Un algoritmo nuevo y original depende de que nadie más lo conoce. La protección del Secreto de Mercado permite la distribución del resultado de un secreto (la parte del ejecutable) mientras se mantiene el diseño del programa escondido. Pero, el Secreto de Mercado nos cubre igual que los Derechos de Autor, así que el secreto no puede ser protegido en contra de piratas que venden copias del programa de alguien sin su permiso. Algo que si cubre es el robar el secreto y utilizarlo en otro producto.

La protección del Secreto de Mercado no sirve de mucho cuando alguien infiere el código estudiando su salida, o decodificado el código objeto. Ya que ambos son actividades legítimas y causan que el Secreto de Mercado desaparezca.

	Derechos de Autor	Patente	Secreto de Mercado
Lo que protege	Expresión de una idea, no la idea misma.	Inventos, la manera en como funcionan.	Información que permite tener una ventaja competitiva.
Protección de forma pública.	Si. Su intención es promover la públicación.	Diseño archivado en una oficina de Patente.	No
Distribución	Si	No	No
Protección Legal	Se puede demandar si una copia es vendida	Se puede demandar si la invención es copiada	Se puede demandar si la información es obtenida de una forma inadecuada.

1.5. Protección de Objetos de Cómputo

En el apartado anterior di un breve esbozo de las formas de protección legales para los objetos relacionados con la computación, ahora describiré como se aplican.

Protección de Hardware

Tanto los chips, como los drives, o los discos de almacenamiento pueden ser patentados al igual que toda la computadora, y si alguien inventa un nuevo proceso de manufactura también puede obtener una segunda Patente.

Protección del Firmware

La situación se hace menos clara con lo concerniente al microcódigo. Si bien los mecanismos físicos en los que el microcódigo es almacenado pueden ser patentados, como es el caso de un chip de propósito especial que realiza una tarea especifica (como es el obtener el punto flotante). Los datos (instrucciones, algoritmos, microcódigo y programas) que están contenidos en los mecanismos, generalmente no son patentados.

Lo ley de protección más apropiado para este tipo de mecanismo, sería el Secreto de Mercado.

Protección del Código objeto.

El código objeto generalmente es copiado y puede ser distribuido para obtener ganancias. El código es un trabajo de creatividad, y la distribución del código es una forma aceptable de públicación, por lo que los derechos del Derechos de Autor, parecen ser lo más apropiado.

Protección del código fuente

Los desarrolladores de software que venden al mercado en masas se niegan a distribuir su código fuente. El código puede ser tratado como un Secreto de Mercado, aunque también se podría aplicar la ley del Derechos de Autor.

Protección de la documentación

La protección de Derechos de Autor es efectiva y apropiada para la documentación debido a que se trata de documentos escritos. Un programa debe ser registrado ante Derechos de Autor de forma separada de su documentación.

Derecho de empleado y Contratantes

Las empresas contratan empleados para generar ideas y hacer productos. La protección ofrecida por Derechos de Autor, Patentes y Secreto de Mercados aplican a las ideas y productos. Pero el considerar quien el dueño de la idea es más complejo. La propiedad es una característica de la seguridad en cómputo, porque se relaciona con los derechos de un patrón a proteger la confidencialidad e integridad de los trabajos productos elaborados por sus empleados.

1.5.1 Propiedad de los productos.

Al interpretación de la ley de propiedad es muy difícil ya que se tienen que considera varios aspectos como:

- La capacitación dada al empleado
- El tiempo laboral que dedico para elaborarlo (en su casa o en el trabajo)
- La idea de elaboración.

La persona que tiene la propiedad de un trabajo patentado es el inventor. Si la empresa lo permite el empleado es quien puede patentar el invento, pero generalmente es la empresa quien lo patenta porque es ella quien el paga al empleado para que realice el invento.

Los derechos de Derechos de Autor son muy similares a los de la Patente. Sin embargo se aplica la situación de trabajo "Bajo Contrato" para el desarrollo de software y otros productos.

Una alternativa para el arreglo de trabajo Bajo Contrato, son las Licencias de Software. En esta situación, el programador desarrolla y retiene toda la propiedad del software. Bajo una tarifa el programador obtiene una Licencia para usar el programa. La Licencia puede ser por un período definido o ilimitado, por una copia

o por un número ilimitado de copias para usarse en un sólo lugar o en varios, en una máquina o en varias, por una o varias veces. Este arreglo suele tener muchas ventajas para el programador.

Cuando existe un trabajo bajo contrato, es el contratante y no el empleado es considerado el autor del trabajo. Esta relación no es muy simple de identificar. Un contratante puede estar en condiciones de trabajo bajo contrato cuando se presentan las siguientes condiciones:

- El empleado tiene un supervisor que vigila la forma en como se esta desarrollando el trabajo.
- El contratante tiene el derecho de despedir al empleado.
- Un contrato escrito entre el contratante y el empleado establece que el contratante ha contratado al empleado para realizar cierta actividad.

Un contrato especifica que el empleado es contratado para trabajar como un programador exclusivamente para beneficio de la empresa. La compañía establece que todos los derecho sobre todos los programas desarrollados, incluyendo los Derecho de Autor y el Secreto de Mercado. El contrato también puede especificar que el empleado esta recibiendo acceso a cierta información clasificada como parte de su trabajo, y que el empleado esta de acuerdo en no revelar esos secretos a nadie.

1.6. Características Legales de la Información

En forma gradual, los servicios se han convertido en cosas mensurables, casi como los objetos. Algunos de ellos tiene un precio fijo, los prestadores de servicio de alguna manera lo que venden es tiempo. El valor de un servicio en una economía libre es de alguna forma relacionado con demanda del comprador y el vendedor del servicio.

Es indiscutible el valor pecuniario que tiene la información. En los negocios se paga por un reporte de crédito, un listado de clientes e información interna de los competidores.

Así como las cosas tangibles y los servicios, la información puede ser vendida y revendida. Un bufete de crédito puede vender el mismo reporte de crédito a un número ilimitado de solicitantes. Los clientes pagan por la información en el

reporte. El reporte puede ser dado en algún medio tangible, como papel, pero es la información y no el medio lo que vale.

Esta cualidad separa la información de otros trabajos creativos como los libros, discos compactos, o arte impreso. Cada uno de estos es algo tangible, que pueden ser numerados o inventariados. Una librería puede vender libros y cada venta significa una reducción en el inventario, así que sólo pude vender tantas copias como tenga en existencia. Lo que no sucede con la información.

El valor de la información es lo que el comprador pagará al vendedor. Pero después de haber adquirido la información el comprado se puede convertir en vendedor y potencialmente hacer que el vendedor original deje de vender. Debido al primer inciso de que la información no esta sujeta a inventario.

El valor de la información depende mucho del tiempo, si alguien conociera información que la semana que entra causara que el precio de algo suba o baje. Esa información seria tan valiosa como si se conociera el precio exacto. Por lo que esta información seria vendida a un precio muy alto.

La información es transmitida vía bits a través de un cable. Si la información es visiblemente dañada (si el detector de error indica un error de transmisión), es fácil demostrar ese error, pero si la transferencia llega intacta y la información fundamental es incorrecta, como se puede justificar que la información esta dañada.

La ley trabaja de una forma muy razonable, aunque un poco retardada, respecto a esta nueva área. El comercio electrónico, la publicidad electrónica, la votación electrónica, el banco electrónico: todos estos son nuevos retos al sistema legal.

1.6.1 Comercio de Información.

La información es un bien en el mercado. Tiene un valor y puede ser la base de un comercio. El mercado aun es joven y algunos problemas se han presentado.

La piratería del software es el primer ejemplo en que el valor de la información puede ser copiado. Varios estudios han tratado de asegurar que el desarrollador de software o quienes la públican reciben la compensación justa por el uso del software.

1.6.2 Públicación Electrónica

Tanto las noticias como la información son públicadas y distribuidas en Internet o alguna otra red pública. Aquí viene otra vez el problema de asegurar que quien la pública reciba la compensación justa por su trabajo.

1.6.3 Protección de Datos en una Base de Datos

Ha existido dificultad para interpretar las leyes de protección para las bases de datos. Por qué como se puede determinar que un conjunto de datos viene de una base de datos en particular.

1.6.4 Comercio Electrónico

Si se trata de hacer compras electrónicamente, las firmas digitales y otros protocolos criptográficos pueden proveer de protección técnica para el dinero de la compra. Pero suponiendo que la información que se ordeno no esta disponible para su uso, o nunca llego, o llega dañada o llega muy tarde para usarse. ¿Cómo se puede probar que se envió, y que llegó bien?

1.7. Crímenes y Criminales

Las leyes relacionadas a los contratos y empleados es difícil, pero por lo menos tanto los objetos como los contratos y los propietarios son entidades para las cuales existen precedentes legales. En cambio los crímenes que se relacionan con computadoras están en un área de la ley que es menos clara que las otras. Por lo que si con las características anteriores las leyes se tienen que adecuar para caber dentro de estos nuevos objetos. Con respecto a los crímenes se debe considerar crear nuevas leyes.

El crimen se clasifica de gente y otros objetos. Se considerara crimen a un acceso no autorizado a un sistema de cómputo.

Hasta ahora ha sido claro, que la comunidad legal no se ha podido acomodar a los avances en la tecnología de la manera en que el resto de la sociedad lo ha hecho. Algunas personas en el proceso legal no entienden de computadoras ni de computación, así que no están capacitados para darle un seguimiento adecuado a los crímenes que se comenten en contra de los sistemas de cómputo. El crear y

cambiar las leyes es un proceso lento; y si se le agrega el dinamismo con el que cambia la tecnología, este proceso se retarda aún más. Otro concepto que se debe considerar, es que la computadora puede tomar varios roles en un crimen:

- Una computadora puede ser objeto, medio o sujeto de un crimen.
- Una computadora puede ser atacada, utilizada para atacar o para realizar un crimen.

Algunas de las principales razones por las que los crímenes computacionales son difíciles de determinar son:

- *Comprensión.* Ni las cortes, ni los abogados, ni los policías, o el jurado son muy sabios en cómputo.
- *Huellas.* Policías y la corte por años han dependido en evidencias tangibles, tales como las huellas de los dedos.
- *Bienes.* El robo de 1 disquete con información valiosa no es lo mismo que el robo de un diamante.
- *Jóvenes.* Muchos crímenes se relacionan con jóvenes y sus crímenes se toman como una inmadurez, sin dárseles un seguimiento adecuado.

Las víctimas de los crímenes analizando la situación en la que se encuentra la ley, prefiere no acudir a ella, porque en muchos casos sería una pérdida de tiempo además de que pocos abogados conocen del tema y podría ser muy difícil y costoso llevar un juicio. Sin mencionar la publicidad negativa que se generaría en su contra, donde el publico perdería la confianza en sus sistemas de cómputo y por lo tanto en ellos.

Muchos de los ataques mencionados caen en la categoría de crímenes y esto va a depender en quien los comete y las intenciones que pueda tener. A veces estas categorías se traslapan.

1.7.1 Perfiles de Criminales.

- Crackers, su principal motivación es el accesar un sistema o datos

- Criminales, ganar dinero

  ◊ Fraudes y abusos
  ◊ Espionaje

- Vándalos, causar daño

  ◊ Usuarios autorizados
  ◊ Extraños a los sistemas

Aunque los tres grupos de perpetradores se pueden considerar criminales, la categoría típica de criminal se enfoca en cuatro tipos principales de conducta criminal: espionaje, vandalismo, reto intelectual, abuso y fraude.

1.7.1.1 Espionaje

Los sistemas de cómputo almacenan y procesan la información nacional más delicada, así como secretos industriales. Esta categoría de crímenes incluyen espías internacionales que roban secretos de la defensa, académicos e investigaciones de laboratorio. Incluye criminales que roban información de las agencias de inteligencia, o agentes de espionaje que operan para la competencia o gobiernos extranjeros que pagan por este tipo de servicio.

1.7.1.2 Abuso y Fraude

Fraude computarizado y abuso son dos ramas crecientes en la industria. Tanto individuos como organizaciones tienen mucho trabajo en estas áreas. En larga escala, muchas organizaciones criminales trabajan con el crimen computarizado y manejar dinero proveniente del narcotráfico. La razón de esto se debe a la cantidad de dinero que pueden ganar y los pocos riesgos que esto conlleva.

1.7.1.3 Vándalos

Los criminales de cómputo en la categoría de vándalos no cometen sus crímenes por estimulación intelectual, por ganancia política o financiera. Generalmente la gente que esta dentro de esta categoría esta enojada, con alguna organización en particular, pero las más de las veces con ellos mismos y la sociedad.

Los vándalos pueden dividirse en dos grupos, a los que llamaremos usuarios e intrusos. Los usuarios son los que están autorizados a usar el sistema y comente abusos con este privilegio. Los intrusos son los que no tienen autorización para utilizar el sistema de ninguna forma:

- Usuarios

  En este grupo están los usuarios autorizados que realizan

operaciones no autorizadas. Los usuarios en esta categoría pueden buscar dañar información o verla antes de irse, esperando recibir un pago por ella de algún competidor, incluso pueden utilizar sus habilidades par causar más daño.

- Intrusos

  Aquí se encuentran los usuarios que no tienen autorización para accesar el sistema.

1.7.1.4 Reto Intelectual

Aunque parezca increíble, en este grupo están los que son atraídos por lo que llaman "reto intelectual" que representa el accesar un sistema para el que no tienen autorización. Ellos mismos se ven como disconformes con el sistema establecido. Generalmente operan de noche, porque durante el ida o están en la escuela o realizan actividades que no les satisfacen del todo.

Muchos de estos perpetradores son adolescentes, que pueden penetrar sistemas de todo tipo.

Algunos crackers operan en grupos, pero muchos lo hacen de forma solitaria. A pesar de que son gente muy inteligente tienen poco rendimiento en la escuela o en el trabajo. Algunos de ellos tienen pocos amigos, además de los que les ayudan a sus actividades crackers. Su mayor forma de interacción humana puede ser boletines de computadora que intercambian con otros crackers.

Aunque muchos son motivados por ganancia personal, otros lo hacen por reto intelectual o alguna forma de atacar el sistema.

Los grupos de crackers tienden a ser informales. Y como se menciono antes aunque muchos lo hacen por diversión o reto intelectual otros lo hacen para conseguir un puesto en alguna compañía y a la rentabilidad de accesar sistemas federales o financieros, ésta actividad se ha vuelto muy redituable.

1.7.2 Características de los Criminales en Cómputo.

Las características de los criminales en cómputo están divididas en cuatro categorías que son:

- Características de Organización
- Características de Operación
- Características Comportamiento
- Recursos

Características de Organización	
Organización	Los espías y el crimen organizado tienen estructuras de organización muy fuertes, que les permite realizar grandes crímenes.
Reclutamiento	Más que lo crímenes comunes, el crimen de cómputo ofrece más atracciones que va de pura codicia hasta un reto intelectual.
Conexiones Internacionales	Tanto los crackers y los agentes de espionaje suelen tener conexiones internacionales. El cracker necesita conexiones con quien compartir los retos intelectuales. El espía necesita comunicarse con la gente con la que trabaja o para la que trabaja.
Características de Operación	
Planeación	En muchos casos, los criminales de cómputo son planeados meticulosamente. En otros casos las oportunidades se presentan así mismas debido a que las organizaciones no presentan medidas precautorias, y los criminales toman ventaja de la situación.
Nivel de Experiencia	Aunque el nivel de experiencia varia, muchos criminales están altamente capacitados y con amplios conocimientos.
Tácticas y métodos usados.	Las tácticas varían dependiendo del motivo y el nivel de experiencia.
Características de Comportamiento	
Motivación	La motivación va desde el dinero hasta la diversión. En otros casos puede existir un factor emocional, como cuando un

	empleado esta molesto con su empresa.
Características personales	No es exactamente un perfil de personalidad, pero designa el tipo de inteligencia o algunas características que el criminal en diferentes categorías puede poseer.
Debilidades Potenciales	Para atrapar un criminal es necesario ver le potencial de debilidad que puede poseer cada criminal. Se debe considera que algunos crackers no consideran que lo que hacen cae en la categoría de crimen. Incluso hay algunos que se consideran héroes por ayudar a la sociedad a identificar sus vulnerabilidades. Generalmente los criminales de cómputo, como otros tipos de criminales son atrapados cuando se vuelven demasiado codiciosos o descuidados. Su misma confianza en ellos les hace dejar pistas.
Recursos	
Entrenamiento	Mientras más entrenamiento tengan mayor es la experiencia. Este entrenamiento va desde un entrenamiento formal hasta adquirir experiencia sobre la marcha.
Equipo mínimo requerido	Muchos crímenes se comenten con lo que llamaríamos el equipo básico: una computadora y un módem. Con el que pueden accesar al objetivo, si no tiene la protección suficiente. Pero si así es requerido, como en el caso de las comunicaciones electrónicas se adquiere el equipo indispensable.
Soporte estructural	Entre criminales necesitan retroalimentación o alguien que les ayude a cometer sus fechorías, en el caso de los crackers reciben apoyo de otros crackers, con los espías reciben apoyo de los gobiernos o la competencia. Muchos criminales simplemente trabajan por si mismos, sin ninguna estructura de soporte.

De acuerdo al cuadro anterior la forma en que operan los criminales de las computadoras se agrupan de la siguiente manera:

Características de Organización

Ofensores	Organización	Atracción	Conexiones Internacionales
CRAKERS			
Grupos	Organizaciones no estructuradas, contraculturales	Atracción de grupo	Interactuan con gente al rededor del mundo
Individuos	generalmente son muy solitarios	Reto intelectual	Se suscriben a jornadas de crackers o intercambian información el los BBS
CRIMINALES			
Espías	Apoyados por agencias de Inteligencia	Su atracción principal es el dinero, en otras lo hacen por razones ideológicas	Utilizan redes para penetrar un objetivo alrededor del mundo.
Fraudes y Abusos	Suelen operar como pequeñas organizaciones o suelen cometer el fraude sólos	Dinero y poder.	Utilización servicios de transferencia electrónica para transferir el dinero.
VANDALOS			
Intrusos	Generalmente son gente joven, que actúa sólo o en grupo	Venganza, reto intelectual, dinero	Utilizan redes y sistemas telefónicos para penetrar en sus objetivos.
Usuarios	Por los usual son empleados	Venganza, poder, reto intelectual, gente enojada	ninguno

Características de Operación

Ofensores	Planeación	Nivel de Experiencia	Tácticas y Métodos utilizados
CRAKERS			
Grupos	Planeación detallada	Alta	Se introducen a las computadoras vía red. Intercambian información con otros crackers y grupos.
Individuos	Estudian los objetivos antes de realizar los atentados	Mediana y alta. Experiencia ganada a través de redes sociales	Utilizan ensayo y error
CRIMINALES			
Fraude y Abuso	Mismas características que los crackers	Mediana a alta, aunque poseen más experiencia en fraude y abuso que en cuestiones computacionales	Utilizan medios de intrusión como el tapar las redes y puertas falsas.
Espionaje	Mismas características que los crackers	Alta	Pueden contactar crackers para recolectar su información o conocer métodos de acceso.
VANDALOS			
Intrusos	No tienen planeación.	Varia	Merodean hasta que se pueden accesar el sistema
Usuarios	Tiene una planeación detallada	Varia. Puede tener un alto nivel de experiencia	Puertas falsas, caballos de Troya. Modificación de datos.

Características de Comportamiento

Ofensores	Motivación	Características Personales	Debilidades potenciales
CRAKERS			
Grupos	Reto Intelectual, diversión, apoyo a una causa	Individuos altamente inteligentes, contracultura	No consideran sus actos como crímenes. Hablan libremente de ellos.
Individuos	Reto intelectual, resolver el problema, poder, dinero, apoyo a una causa	Inteligencia moderadamente alta	Puede mantener notas y otros documentos que lo inculpan
CRIMINALES			
Espionaje	Dinero	Pueden ser crackers que operan en grupo o individuos	Se vuelven ambiciosos de la información, lo que les hace cometer errores.
Fraude/abuso	Dinero u otras ganancias personales	Las mismas características que algunos ofensores fraude.	Se vuelve ambicioso lo que les hace cometer errores.
VANDALOS			
Intrusos	Cambio intelectual, dinero, poder	Mismas características que los crackers	Se vuelven muy descuidados y cometen errores.
Usuarios	Venganza en contra de las organizaciones	Los usuarios tiene alguna experiencia en cómputo	Dejan rastros en los archivos de registro de las máquinas

Recursos

Ofensores	Habilidades	Equipo mínimo necesario	Estructuras de soporte
CRAKERS			
Grupos	Alto nivel de entrenamiento informal	Equipo básico de computadora con módem	Soporte de grupo
Individuos	Experiencia ganada a través de la experiencia	Equipo básico de computadora con módem	BBS
CRIMINALES			
Espionaje	Varios niveles de experiencia	Equipo básico de computadora con módem, en algunas ocasiones es necesario equipo más sofisticado	Agencias de Inteligencia
Fraude/abuso	Experiencia programando	Computadora con módem o acceso a la computadora objetivo	Grupos.
VANDALOS			
Intrusos	Van desde habilidades básicas hasta gente altamente preparada	Acceso a las computadoras objetivo	Ninguno
Usuarios	Experiencia en computación.	Acceso a la computadora objetivo	Ninguno

La cantidad de información financiera, militar, de inteligencia, de negocios, de investigación, y personal que es almacenada y transmitida día a día por medio de computadoras es inimaginable.

Los gobiernos, la industria militar y económica actualmente no podrían operar sin la computación automatizada. Las computadoras están ligadas vía Internet o redes militares o financieras.

Toda la información que esta almacenada o que es transmitida es susceptible de ataques y casi toda organización ha sido afectada por algún crimen. El constante incremento de redes interconectadas hace que los crímenes sean más fáciles. Motivos que hacen necesaria que los gobiernos presten más atención a este reto tecnológico en el que todos estamos envueltos.

CAPITULO II

Medidas Preventivas

La Seguridad de todos los recursos de cómputo, es un aspecto primordial en toda organización que todos los profesionales del área, administradores y usuarios de todos estos recursos deben tener presente. Algunas de estas organizaciones ya están conscientes del valor que resguardan en sus instalaciones (equipo e información) y tienen sistemas de seguridad muy estrictos y eficientes; pero existen otros muchas, que parecen no asimilarlo hasta que padecen algún ataque.

En el primer capítulo hablamos de como la seguridad de un sistema se ve afectada, en primera instancia por vulnerabilidades que se convierten en amenazas latentes (si no son detectadas y corregidas a tiempo) y por lo tanto en posibles ataques.

Un sistema de cómputo es una colección de hardware y software, medios de almacenamiento (discos duros, disquetes, cintas, etc.), datos y personas; y cualquiera de estos recursos puede ser el objetivo de un crimen.

Los crímenes más comunes se refieren a interrupción, intercepción, modificación y falsa fabricación:

- Una interrupción, es cuando un bien se pierde, no esta disponible, esta dañado o es inservible.
- Intercepción, es cuando personas no autorizadas tiene acceso a un bien.
- Modificación, cuando no sólo se logra la intercepción sino también se hacen cambios en la información.
- Falsa fabricación de información en lo sistemas.

2.1 Análisis de Riesgos

La planeación de la seguridad empieza con un análisis de riesgos. El análisis de Riesgos es un proceso para determinar las amenazas y sus daños potenciales. Se inicia con una lista de todas las vulnerabilidades del sistema. Después, para cada amenaza, se plantean una serie de medidas preventivas, así como el costo que representaría aplicarlas. El último paso es un análisis costo-beneficio es preguntar: ¿qué cuesta menos, implementar un control o aceptar los riesgos?.

El análisis de riesgos lleva a un plan de seguridad, que identifique acciones que tomen la responsabilidad de evitar ataques.

Un análisis de riesgo, como su nombre lo implica, es un estudio de los riesgos de hacer algo. Algunos riesgos son simplemente parte del costo de los negocios, en algunas ocasiones se toma como parte normal de la operación.

Las medidas preventivas pueden reducir la seriedad de una amenaza. Las empresas muy grandes que tienen centros de cómputo en muchos lugares, no pueden determina fácilmente los riesgos y las medidas que deben ser tomadas en sus centros de cómputo.

2.1.1 Razones para Realizar un Análisis de Riesgo

Algunos de los beneficios que un buen análisis de riesgo son:

- *Usuarios conscientes.* El hacer público las características de la seguridad y los beneficios de esta, hace que los usuarios se vuelvan más conscientes y cooperen con las medidas tomadas, fortaleciendo con esto la seguridad.

- *Identificar los bienes, sus vulnerabilidades y las medidas de seguridad.* Algunas empresas no saben que las información que manejan, sin la menor precaución puede representar un riesgo muy grande para sus estabilidad. Un análisis sistemático produce una lista de la información importante que tiene riesgos y debe ser protegida.

- *Mejorar las decisiones básicas.* En ocasiones la productividad se decrementada, por las medidas excesivas de control y las inconveniencias de los usuarios. También, algunos riesgos no pueden ser justificados desde la perspectiva de protección que proveen, por lo que se tiene que buscar otra forma de control, menos problemáticos.

- *Justificar los gastos para obtener seguridad.* Muchas medidas de seguridad son muy caras y no tiene ningún beneficio importante. Un análisis de riesgo pude ayudar a identificar los casos que valen la pena el tener este tipo de seguridad.

2.2.2 Pasos de un Análisis de Riesgo.

El análisis de riesgo es un proceso ordenado, que se tiene que dar en el manejo de sistemas. Muchos de los puntos son flexibles para ser adaptados a cada sistema de cómputo, porque no todos tiene que proteger el mismo tipo de información o tiene las mismas debilidades.

Los pasos básicos son:

1) Identificar los bienes importantes a ser protegidos

Este es el primer paso a ser tomado en un análisis de riesgo es el identificar los principales puntos de ataque de un sistema. Algunos ya los describimos en las principales vulnerabilidades de los sistemas de cómputo.

- *Hardware:* procesadores centrales, tarjetas, teclados, monitores, terminales, microcomputadoras, estaciones de trabajo, unidades de lectura-escritura, impresoras, cables, conexiones, controladores de comunicaciones y medios de comunicación.

- *Software:* programas fuente, programas objeto, programas de utilidad, sistemas operativos, compiladores y programas de diagnóstico y mantenimiento.

- *Datos: Los* datos utilizados durante la ejecución, los datos almacenados en medios magnéticos, los datos impresos, los datos archivados, los registros de auditoría, etc.

- *Documentación:* La documentación de programas, hardware, sistemas, procedimientos administrativos y de todo el sistema.

- *Materiales:* papel, formas, cartuchos láser, medios magnéticos, etc.

- *Gente:* La gente que se encarga de correr los procesos o almacenar información, administrar los recursos.

Un análisis de riesgos empieza con una lista de todos los bienes que componen un sistema de cómputo. Digamos un inventario del sistema.

1) Determinar las Vulnerabilidades

El hacer la lista de los bienes que componen el sistema, es relativamente fácil, porque muchos de estos bienes son tangibles o fácilmente identificados. El siguiente paso del análisis de riesgos es determinar las vulnerabilidades de esos bienes. En este paso se necesita visualizar la situación desde muchos ángulos y perspectivas, para poder hacer una predicción de los daños que pudieran ocurrir, quienes estarían en posibilidad de efectuarlos y bajo que circunstancias.

El capítulo primero lo iniciamos enunciando las características que debería tener un sistema para ser seguro, Confidencialidad, la Integridad y la Disponibilidad. Una amenaza es la posible pérdida de algunas de estas tres características. Las posibles vulnerabilidades pueden ser identificadas considerando las situaciones que pueden causar pérdida de la confidencialidad de un objeto, la pérdida de integridad o la pérdida de disponibilidad.

A continuación se presenta una tabla en las que se pueden organizar los bienes y anotar las posibles amenazas que los podrían afectar de acuerdo a las 3 características de seguridad, esta tabla, al igual que la Lista de Evaluación no es rígida, y se puede adecuar a las características de cada sistema.

Bien	Confidencialidad	Integridad	Disponibilidad
Hardware			
Software			
Datos			
Gente			
Documentación			
Materiales			

Y las preguntas a considerar son:

- ¿Cuáles son los efectos de errores no intencionales? Por ejemplo, teclear el comando equivocado, datos equivocados, borrar la información equivocada, etc.

- ¿Cuáles serían los efectos de intrusiones premeditadas, por parte de gente interna a la empresa? Considerando a los empleados descontentos o ambiciosos.

- ¿Cuáles serían los efectos para intrusos externos? Pensando en acceso por medio de red, acceso vía módem, crackers, gente que busca en la basura, etc.

- ¿Cuáles serían los efectos de accidentes naturales? Fuego, tormentas, inundaciones, descargas eléctricas o fallas del equipo.

Al llenar la tabla con la respuesta a éstas preguntas, nos muestra los problemas más comunes que pueden afectar el sistema.

3) Estimar la probabilidad de explotación de estas debilidades

El paso tres del análisis de riesgo es determinar las probabilidades de que una amenaza se convierta en un ataque al sistema. La probabilidad va a ser el resultado del tipo de amenaza, la facilidad con la que sería detectada por los atacantes y la posibilidad de que sean burladas las medidas de control tomadas para disminuir los riesgos. Puede que algunos eventos sean imposibles de pronosticar, de cualquier manera existen métodos por los que la probabilidad de que un ataque ocurra pueda ser calculada.

- Probabilidad, existe información por la que se puede determinar las posibilidades de que un empleado cometa fraude, robo o algún otro crimen, así como de posibles errores intencionales o no. También se puede hacer una encuesta de un determinado sistema, para localizar sus posibles fallas en los sistemas operativos, en el hardware, en los intentos fallidos de conectarse con identificaciones falsas, el número de accesos, el tamaño de los archivos y fecha de modificación, etc.:

- Número de ocurrencia en un período determinado. Se le pide al encargado del sistema hacer una relación del número de ocasiones que determinado hecho ocurrió.

- Estimar la probabilidad con la ayuda de una tabla. Elegir un evento y colocar en una tabla un rango de ocasiones en las que pudiera ocurrir y entonces registrar un porcentaje de acuerdo a este número.

4) Estimar el tamaño o los efectos de la posible pérdida

Estimar el costo estimado de cada ataque es el siguiente paso en la realización de un análisis de riesgos. Así como la probabilidad de ocurrencia, este

valor también es difícil de determinar. Algunos costos, como el de reemplazar una pieza de hardware, es fácil de determinar, incluso el costo de remplazar una pieza de software es fácil de obtener, pero el valor de los datos no se calcula tan fácilmente, porque son muchos intereses los afectados.

Algunos datos necesitan ser protegidos por razones legales. Los datos de índole personal, como la información de impuestos, datos del censo, información médica. La información referente a la empresa es confidencial, por ejemplo los datos de un nuevo producto, resultados de ventas, o algún tipo de información financiera que pudieran dar a la competencia ventaja competitiva. Algunos datos financieros, especialmente los adversos a la economía de la empresa, pueden afectar de forma negativa a la organización si su rubro es el manejo de dinero, como el caso de los bancos, las aseguradoras, las casas de bolsa. Así que por lo visto anteriormente, realmente resulta difícil valuar los datos.

En un sistema de cómputo, una pieza de software, o una clave personal son incalculables, ya que pueden ocasionar que un servicio se retrase, provocando grandes pérdidas.

Las siguientes preguntas puede llevar a un análisis de ramificaciones de una falla de la seguridad del sistema de cómputo. Las respuestas a estas preguntas pueden ayudar a identificar los costos.

- ¿Qué obligaciones legales existen para preservar la confidencialidad y la integridad de los datos?
- El divulgar determinada información, ¿podría de alguna forma causar daños a una organización o a un particular?
- ¿Existe la posibilidad de alguna acción legal?
- ¿Podría algún acceso no autorizado a la información causar algún daño en una futura oportunidad de negocio de la empresa?
- ¿Podrían los competidores ganar una ventaja desleal?
- ¿Cuál sería el daño estimado?
- ¿Cuál sería el efecto psicológico de la falta de servicio de cómputo?
- ¿Cuántos clientes serían afectados?
- ¿Cómo se vería afectada la productividad?

- ¿Qué valor tiene el accesar determinados datos o programas?
- ¿Podrían ejecutarse después los procesos, o en algún otro lugar o alquilar otro equipo?
- ¿Qué costo tendría el ejecutarse después o en algún otro lugar, o con otro equipo?
- ¿Qué problemas traería la pérdida de información?
- ¿Sería remplazada o reconstruida?
- ¿Cuál sería el costo de reemplazarla o reconstruirla?

Como mencione, estos costos no son fáciles de evaluarse. Sin embargo, deben ser evaluados para determinar el daño que podría ser causado. Las amenazas en la seguridad de cómputo, suelen ser poco valoradas. Estimaciones reales del daño que puede ser potencial, eleva la preocupación de la seguridad en cómputo e identifica los lugares donde debe existir atención especial.

El costo de un incidente es determinado, utilizando la guía anterior. Pero el costo generalmente es estimado por año, por lo que este deber ser multiplicado por el número de incidentes por año.

5) Buscar las posibles medidas de control y sus costos

Los cálculos reflejan la situación de una empresa en un momento determinado, y si estos cálculos reflejan una pérdida considerable, es tiempo de cambiar las medidas de seguridad o implementar unas.

Una forma de identificar las medidas de control adecuadas para cada amenaza es revisando la lista de medidas preventivas :

- Controles de encriptación
- Protocolos de seguridad
- Programas de control de desarrollo

- Programas de control de ambiente de ejecución
- Protección de los sistemas operativos
- Identificación
- Autenticación
- Control de acceso a las bases de datos
- Controles de inferencia de las bases de datos
- Multiniveles de control de seguridad para los datos, las bases de datos y los sistemas operativos
- Controles de computadoras personales: procedimientos, protección física, protección de hardware y software
- Control de acceso de red
- Control de integridad de las redes
- Controles físicos ...

6) ¿Cuáles serían los beneficios de estas medidas de control?

Para finalizar el análisis de riesgos, es conveniente realizar un análisis de costo-beneficio de las medidas de control para prevenir los ataques.

Primero se tiene que obtenemos la pérdida anual y le restamos el porcentaje en que se reduce la pérdida esperada más el costo de las medidas. Por lo que el costo efectivo, podría ser negativo si la reducción del riesgo es mayor que la del control.

Ejemplo:

Bien	Riesgo
Acceso no autorizado a datos y programas: $100,000 * 2% de probabilidad por año.	$100,000
Efectividad de las medidas de control: 60%	-$60,000
Costo de acceso al software preventivo	$25,000
Costo anual esperado debido a pérdidas y medidas de control: $100,00-$60,000+25,000	$65,000
Ahorro:$100,000 -$65,000	$35,000

2.2 Plan de seguridad

Un plan de seguridad es un documento que describe como una organización plantea sus necesidades de seguridad. El plan deber sujetarse a revisiones periódicas, según las necesidades de seguridad vayan cambiando.

Un buen plan de seguridad es un documento oficial que las actuales prácticas de seguridad. También identifica un plan hacer cambios o mejorar esas prácticas de una manera estructurada. Por lo que, también puede ser útil para medir el efecto de los cambios, y sugerir otras mejoras. El impacto del plan de seguridad también es muy importante.

Los aspectos que debe cubrir un plan de seguridad son:

1. Que debe contener un plan
2. Quien escribe el plan
3. Como adquirir soporte para el plan

El plan debe identificar y organizar las actividades de seguridad para un sistema de cómputo; además, abarcar la situación actual y los cambios proyectados, a través de los siguientes aspectos:

2.2.1 Políticas

Deben indicar el fin primordial de los esfuerzos de seguridad. Durante esta fase se plantean tres preguntas:

- ¿A quién se le permitirá el acceso?
- ¿A qué recursos podrán tener acceso?
- ¿De qué forma será regulado el acceso?

Las políticas de seguridad deben especificar:

- Las metas de seguridad de la organización, por ejemplo, integridad de los datos, evitar la pérdida de información debido a accidentes, etc.
- En quien cae la responsabilidad de las acciones de seguridad, listando el nombre de la persona, su puesto y las actividades que esta persona realiza.

2.2.2 Estado Actual

Describir el estado de la seguridad al momento de elaborar el plan. Un análisis de riesgo puede estar conformado con una descripción de la situación actual de la seguridad. Esta situación incluye una lista de los bienes de la organización que necesitan protección, las posibles amenazas, y las medidas precautorias.

El plan debe definir limites de responsabilidad: especificar los bienes deben ser protegidos; que grupos son excluidos, en el caso de que sea una empresa que tiene contacto con otras organizaciones vía red; y el perímetro de protección de la organización.

2.2.3 Recomendaciones y Requerimientos.

El corazón de los planes de seguridad son las acciones que deben ser tomadas y los requerimientos que serán necesarios para cumplir con los objetivos de este plan, y en que tiempo deberá ser implementado. Muchos planes no pueden ser llevados a cabo inmediatamente. En algunos casos debe existir un período de implementaron, especialmente si este esta compuesto por fases. EL plan también debe incluir un procedimiento de cambio y crecimiento, de tal forma que los aspectos del cambio será consideradas como parte de preparase para el cambio.

2.2.4 Responsabilidad de Implementación

Una sección del reporte deberá identificar a las personas responsables de la implantación. Por ejemplo:

- Los usuarios de computadoras personales, son responsables de sus máquinas.
- Los líderes de proyectos, son responsables de los datos y procesos de un proyecto.
- Los administradores de las bases de datos, son responsables del acceso y la integridad de los datos en sus bases de datos.
- Oficiales de la Información, serán los responsables de la creación y el uso de los datos; también serán los responsables de la retención y disposición de los datos.

2.2.5 Tiempos de Implementación

Si los controles son caros o complicados, pueden ser adquiridos o implementados gradualmente. Similarmente, los procedimientos de control pueden requerir que el personal encargado de la administración de la seguridad de entrenamiento a los usuarios. El plan deberá especificar el orden en que los controles serán implementados, de tal forma que las amenazas más serias sean cubiertas primero. Este paso, también da una forma para medir el progreso de las medidas implementadas.

2.2.6 Atención Continua.

Una parte importante de la fase de Tiempos de Implementaron, es establecer una fecha, para la evaluación y revisión de la situación de seguridad. Periódicamente el inventario de los objetos y la lista de controles deberán ser actualizados, y el análisis de riesgos serán revisados.

2.3 Encargados de Elaborar el Plan de Seguridad

Dependiendo del tamaño de la complejidad y el tamaño de la organización de cómputo, será el número de personas que se emplearan para elaborar dicho plan. Partiendo de estudios de comportamiento organizaciones, el tamaño óptimo para un grupo de trabajo, es de 5 a 9 miembros.

Los miembros del equipo de planeación de la seguridad, deberán estar relacionados con los diferentes aspectos de la seguridad en cómputo, de los que ya hemos hablado. Finalmente, debido como que las medidas de control afectaran a los usuarios, el plan deberá contemplar el punto de vista de estos, así como algunas sugerencias al respecto.

Como ya mencionamos es recomendable que cada miembro del equipo de seguridad se relacione con alguna de estas áreas:

- Manejo de hardware
- Programadores
- Aplicaciones
- Entrada de datos
- Seguridad personal
- Comunicaciones
- Usuarios

Una vez que el plan es aceptado, lo siguiente es darlo a conocer en la medida en la que afecte a los usuarios. El que los usuarios lo conozcan y sepan como utilizarlo, será parte del éxito; si la gente lo entiende las necesidades de llevar algún tipo de control será poco cooperativa con este.

2.4 Metas de Seguridad

Para que todo sistema se considere seguro debe contar con las características de las que platicamos al principio del capítulo uno y se refieren a la Confidencialidad, Integridad y Disponibilidad. Durante este capítulo veremos algunos métodos, procesos y herramientas que nos pueden ayudar estas metas.

Métodos de Defensa.

Siendo que el objetivo principal es mantener la seguridad en un sistema de cómputo ser recomienda utilizar controles o medidas preventivas que sean capaces de detener los ataques o en el peor de los casos detectarlos.

Medidas Preventivas.

Una vez que conocemos las vulnerabilidades de un sistema, tomar medidas precautorias para que no se conviertan en amenazas, que en determinadas circunstancias afecten de alguna forma el sistema.

Encriptación.

Es la herramienta más efectiva para proveer seguridad a la información que se transmite de un lugar a otro. Funciona transformando los datos de manera que sea absolutamente inteligible para los observadores no autorizados; la gente experta en seguridad de cómputo, puede virtualmente nulificar una intercepción y la posibilidad de una modificación o fabricación de la información mientras esta en transito.

La encriptación permite que los datos sean confidenciales. Otorgando además, la característica de integridad, porque los datos no pueden ser leídos y por consiguiente no son modificados. La encriptación es la base de algunos protocolos, que son una secuencia de acciones para llevar a cabo una tarea. Por

lo anterior, la encriptación es el corazón de los métodos de seguridad en comunicación.

La encriptación es una herramienta importante en la seguridad de cómputo, pero tampoco se debe sobrestimar. Los usuarios deben entender que la encriptación no resuelve todos los problemas de seguridad en cómputo, y si la encriptación no es utilizada de una manera adecuada, puede no tener ningún efecto protector, al contrario puede degradar la funcionalidad del sistema. Utilizar una encriptación débil puede ser peor que no utilizar ninguna, debido a que da una sensación de seguridad que no existe. Conociendo esto es importante conocer las situaciones en las que la encriptación es útil para utilizarlas de una forma efectiva. Debido a la importancia y que hasta ahora es el método que nos garantiza más seguridad, lo trataremos más a detalle en el capítulo siguiente.

Controles de Software.

Los programas son la segunda herramienta importante en cuestiones de seguridad. Los programas deben ser seguros por si mismos para evitar ataques externos. La forma en que son escritos y mantenidos, tiene que ser con la mentalidad de que los usuarios tienen toda la confianza para depender de ellos cuando desarrollan sus actividades:

- *Programas(rutinas) de control interno:* parte del programa que refuercé las restricciones de seguridad, tales como limitaciones de acceso en una base de datos, modificación del programa, etc.

- *Controles de sistemas operativos:* limitaciones reforzadas por el sistema operativo para proteger a los usuarios de intrusos e inclusive de otros usuarios.

- *Controles de desarrollo:* estándares de calidad bajo los cuales un programa es diseñado, codificado, probado y mantenido.

Los controles de software pueden utilizar herramientas como el hardware o la encriptación. Estos controles de software afectan a los usuarios directamente, y en base a ello deben diseñarse con la capacidad de facilidad de uso y funcionalidad.

Controles de Hardware.

Numerosos mecanismos de hardware han sido inventados para ayudar a la seguridad en cómputo. Estos mecanismos van desde tarjetas inteligentes hasta candados

que limitan el acceso de los usuarios.

Políticas.

Muchos controles son simplemente políticas como el cambiar passwords, cada determinado tiempo, que si bien no implican mucho costo si son muy efectivos.

Controles Físicos.

Algunos de los más fáciles y más efectivos y menos caros son los controles físicos. Controles físicos incluyen seguros en las puertas, guardias en las entradas y salidas de las instalaciones donde se resguarda algún recurso de cómputo, copias de respaldo del software así como de los datos más relevantes y una planeación física que reduzca el riesgo de desastres naturales.

Efectividad de los Controles.

El tener controles de seguridad no resulta tan bueno, a menos que sean utilizados apropiadamente. Algunos factores que afectan la efectividad de los controles son:

Las personas que utilizan los controles deben estar conscientes de la necesidad de seguridad, ya que solamente cooperaran si entienden por que la seguridad es importante en cada situación específica.

Probabilidad de Uso.

Ningún control es efectivo a menos que se utilice. El principio de efectividad dice: "Los controles deben ser utilizados efectivamente. Deben ser eficientes, fácil de usarse y apropiados".

Este principio implica que los controles en seguridad en cómputo deben ser suficientemente efectivos, en términos de tiempo, espacio en memoria, actividad humana, u otros recursos utilizados, de tal manera que el uso de los controles no afecte las actividades principales del sistema. Los controles también deben ser selectivos para que no excluyan el acceso legítimo.

Controles Traslapados.

Varios controles pueden aplicarse a la misma amenaza. Si la amenaza es muy grave se pueden utilizar varios controles para prevenirla, siempre con la precaución de que estos controles no se estorben unos a otros.

Revisión Periódica.

Algunos controles son permanentemente efectivos. Cuando los especialistas encuentran la manera de asegurar los bienes en contra de determinados ataques, la oposición redobla los esfuerzos para vencer el mecanismo de seguridad.

Hasta aquí hemos visto el plan de análisis de riesgos ahora veremos algunas de las medidas que pueden ser utilizadas de una manera en aspectos específicos.

Manejo de Seguridad en Computadoras Personales

Desde hace un tiempo el uso de computadoras se ha expandido substancialmente, entre todo tipo de estudiantes, profesionales, comercios y empresas. Utilizamos el termino computadora personal para incluir microcomputadoras, computadoras pórtatiles, etc.

Los usuarios de computadoras personales, no reconocen el riesgo que tienen y por lo tanto no tienen ni la menor idea de como implantar algunas medidas de seguridad para protegerse.

Las aplicaciones que corren en una computadora personal necesitan ser confidenciales, integrales y disponibles al igual que los datos, programas y equipo.

Los problemas de seguridad básicos para una computadora personal son las similares a otros recursos de cómputo de las que ya hemos hablado. A pesar de esto, las herramientas de seguridad no se pueden aplicar a las PC, porque son diseñadas para ambiente multiusuario y red.

Otro peligro importante es el que concierne a las computadoras portátiles (laptops), que en cualquier momento pueden ser robadas, ya sea para venderse como máquina o como información importante.

Generalmente las computadoras no tienen ninguna protección a nivel de hardware y las que tienen no toman ventaja de ellas, por la falta de educación que existe entre los usuarios respecto a la seguridad de sus recursos.

La máquina no es la fuente del problema de seguridad, sino los usuarios de la ésta. La manera en como la gente ve la máquina y sus responsabilidades afectan la seguridad de las computadoras personales.

Los usuarios en general deberían estar capacitados para detectar las vulnerabilidades cuando procesan un texto y almacenan datos en una microcomputadora. Muchos usuarios no consideran estos como riesgos de seguridad y aunque los controles para computadoras personales son menos poderosas, las vulnerabilidades son más numerosas. Algunas vulnerabilidades en la seguridad de computadora personal:

- *Poca preocupación del problema.* Para muchos usuarios, la computadora personal es una herramienta de oficina, análoga a una calculadora o máquina de escribir. La gente que no esta consciente de este problema, son ellos mismos la vulnerabilidad

- *No existe responsabilidad única.* Si una máquina es compartida por varios usuarios, ninguno puede negar la responsabilidad de mantener, supervisar o administrar la máquina.

- *Controles de Hardware.* Algunas computadoras personales toman ventaja de las características del hardware que simplifican la instalación de medidas de seguridad.

- *No existen registros de auditoría.* Cuando surgen problemas, es imposible decir quien ha accesado una máquina y mucho menos cuando.

- *El medio ambiente.* Partículas de humo, bebidas, bajas de electricidad y electricidad estática, pueden causar fallas en las computadoras personales.

- *Acceso físico.* Las máquinas se dejan encendidas, o corriendo procesos o aplicaciones en la oficina. Así que todos los datos contenidos en esa máquina se dejan al alcance de las personas alrededor

- *Falta de cuidado en los medios de almacenamiento.* Disquetes, cintas, etc., que contienen información de software o datos importantes, no son almacenados en algún lugar seguro.

- *Inexistencia de respaldos.* Los usuarios no aprecian la necesidad de hacer constantes respaldos de su información, hasta tienen algún tipo de pérdida.

- *Documentación cuestionable.* El no consultar la documentación de uso de la máquina, puede resultar en accidentes.

- *La Calidad de software poco profesional.* Mucho software para computadoras personales es hecho por personas que no practican las mismas medidas rigurosas de desarrollo o prueba, como lo harían los especialistas y los usuarios en la mayoría veces desconocen el alcance que podría tener este software de dudosa calidad.

- *Retención Magnética.* Cuando se borra un archivo, se borra lógicamente pero no físicamente, y la gente que sabe esto puede buscar en estos medios información que les pueda ser de alguna utilidad.

- *Combinación de actividades.* Es un principio clásico de la auditoría financiera, que ninguna persona tiene responsabilidad total para realizar un transacción completa. En contraste, muchas aplicaciones de computadora personal son diseñadas para que una persona realice todos los pasos.

Aunque la lista de vulnerabilidades es larga y variada, las características que las envuelven las hace caer en tres categorías: uso impropio de

procedimientos, mal uso del hardware y mal uso de software. En cada área existen algunos controles que son razonablemente efectivos. La combinación de controles que dos o más tipos es lo mejor, siempre y cuando no afecte la disponibilidad y eficiencia de los recursos.

Las medidas de seguridad que se pueden tomar para contrarrestar estas vulnerabilidades son:

Medidas Dirigidas a los Procedimientos de Uso

Algunas de las vulnerabilidades identificadas pueden ser controladas por procedimientos administrativos, que son políticas para el uso de máquinas que pueden reducir los riegos asociados con estos recursos descuidados, así como cuidado de medios de almacenamiento, respaldos, el medio ambiente, residuos magnéticos y separación de actividades. Los procedimientos que pueden ser implementados son:

- Nunca dejar computadoras personales sin protección, si estas contienen información sensible o tienen procesos importantes corriendo. El fácil uso de los nuevos paquetes y la estandarización de los mismos en alguna organización, hace que cualquier usuario puede accesar información de máquinas que no tienen ningún tipo de protección.

- Cuando se manda imprimir información sensitiva, no dejar las impresoras solas hasta que termine el proceso. Esta restricción es especialmente importante si una impresora es compartida por dos o más computadoras, o si la impresora esta localizada en un lugar público.

- Mantener los medios de almacenamiento como si fueran reportes confidenciales. Los disquetes que contienen información sensible deben estar guardados bajo llave. Las máquinas con discos duros que tienen información importante deben tener algún tipo de password o estar bajo protección física. Apagar las computadoras después de haber sido utilizadas para limpiar la memoria volátil. Debido a que los datos perduran después de haber sido borrados en algún medio magnético, es conveniente sobreescribirlos primero con ceros, luego con unos y por ultimo con una mezcla de los dos, antes de liberarlos para otros usos. Cuando una computadora personal debe ser enviada para reparación, los discos pueden retener información y si esta información es importante, se podría quitar el disco o se manda arreglar con personal de alta confianza. Si es necesario, copiar el contenido del disco duro a otro medio de almacenamiento y destruir el disco entero.

- Realizar respaldos periódicos. Dependiendo de la importancia de la aplicación, realizar respaldos diarios de archivos cambiados a discos o algún otro medio de almacenamiento. En algunos casos, será mejor hacer respaldos cada vez que un archivo es cambiado. También, hacer respaldos periódicos de todos los archivos así que todo el sistema sea reemplazado en el caso de falla o que existían copias disponibles para cualquier caso de emergencia.

- Practicar las separación de autoridad. Diseñar procedimientos para que ninguna persona tenga toda la autoridad sobre datos importantes. Por ejemplo, en el caso de sistemas de contabilidad, la información se mantenida en dos sistemas por dos personas, y se tenga que hacer el balance entre estas dos personas, lo que dificultaría la posibilidad de fraude hecho por una sola persona

Características Dirigidas a Controles de Hardware.

Además las computadoras personales, no tienen el modo de privilegios de ejecución o protección de memoria a nivel hardware; pero si existen algunas forma de control que dependen de éste, por ejemplo:

- *Seguridad de equipo.* La portabilidad es una ventaja de las computadoras personales, pero esa portabilidad es también una vulnerabilidad. El poner las computadoras bajo cerrojo, o dejarlas en algún lugar que tiene protección física (vigilancia), es una buena forma de dar seguridad contra robo.

- *Protección de acceso.* Diferentes distribuidores de hardware, han diseñado paquetes de control de acceso, para computadoras personales. Algunos de estos paquetes ofrecen sólo control de software, los cuales son fácilmente vencidos o burlados.

- *Algunos paquetes más sofisticados combinan hardware con software.* Aunque estas medidas, también, pueden ser burladas, si pueden proveer de seguridad en contra de ataques casuales.

Características dirigidas a Control de software.

Entre las vulnerabilidades más comunes del software, se incluye la falta de registro de auditoría. El uso de software de fuente no confiables, documentación

pobre, y la falta de control en sistemas operativos, tal como el rehuso de archivos, espacio o control de acceso.

- Utilizar el software con conocimiento de los daños que puede ocasionar. Software de comunicación puede filtrar información, durante su transmisión, los programas que realizan operaciones de cómputo pueden dar respuestas incorrectas y muchos softwares pueden dañar o destruir otros programas o archivos a los que hacen acceso.

- No utilizar software de dudosa procedencia. El software de grandes manufacturadas y distribuidores tiene menos probabilidades de presentar problemas, que el software de pequeños compañías casi siempre desconocidas.

- Comprobar resultados. Progresivamente, las aplicaciones están siendo desarrollados por gente que no es programadora profesional. Estos desarrolladores saben poco acerca de prácticas de ingeniería, como el diseño de métodos, validación de datos y pruebas. La información producida por este tipo de software puede no ser precisa e incluso puede corromper datos de otras fuentes.

Mantener respaldos periódicos de todos los recursos del sistema. En el caso de un accidente debido a fallas de software, la única manera de recuperarlos es reinstalar todo el sistema de las copias de respaldo.

Protección de Archivos

Vamos a dar un panorama general de la protección de los archivos en las computadoras personales. En este contexto tomaremos el archivo como una unidad, y ya sea que se pueda accesar todo el archivo o no se accese ninguna parte.

Esencialmente existen cuatro tipos de protección aplicables a los archivos de computadoras personales:

- El control de acceso, visto como parte del sistema operativo o como paquetes auxiliares

- Encriptación de archivos

- Protección contra copia de información, permitir sólo a determinado grupo de personas a hacer copias de la información.

- No usar ningún tipo de protección, cuando se tiene controlado todo el medio ambiente, la protección sobre los archivos no es necesaria.

Mecanismos de Control de Acceso para Computadoras Personales.

Muchos sistema operativos de computadoras personales no proveen de control de acceso para los archivos; y en donde estos controles están disponibles, la gente no suele usarlos. Esta negligencia resulta del fácil uso de las computadoras y las características del medio ambiente donde operan.

La gran capacidad de los discos, los poderosos sistemas operativos y las redes han creado situaciones en las que varios usuarios pueden compartir productivamente una computadora personal o directorios de la misma. Aun con sólo un usuario por máquina, existen buenas razones para tener mecanismos de control de acceso.

Algunas de las motivaciones para acceder archivos de computadoras personales son:

- *Interferencia externa.* Aun un sistema de un sólo usuario puede ser vulnerable a ser accesado por intrusos, por ejemplo, compañeros de trabajo, personal de servicio de mantenimiento, visitantes y otros que pueden afectar el contenido de un archivo.

- *Dos usuarios para una sola máquina.* No es común que dos compañeros de trabajo compartan una sola máquina. Aunque puede ser razonable asumir que no existe mala intención, un usuario puede destruir inadvertidamente datos o programas que pertenecen al otro.

- *Acceso a red.* Aun en los ambientes de oficina más confiables, conforme las computadoras están conectadas en red, el número de usuarios crece, y la disponibilidad de creer en todos los usuarios decae. Además, los mecanismos compartidos requieren de alguna forma de acceso restringido para asegurar que los recursos sean compartidos sólo con quien deben ser compartidos.

- *Errores.* Protección de acceso puede limitar el efecto de errores restringido los archivos que son accesibles cuando ciertas aplicaciones están corriendo.

- *Software de dudosa calidad.* Mientras un paquete de software no haya sido probado en su totalidad para prever sus efectos sobre otros recursos, es prudente correrlo en un ambiente donde dadas las circunstancias pueda hacer un daño mínimo.

- *Separación por aplicaciones.* Los mecanismos de control de acceso, pueden facilitar la separación lógica de los archivos por contenido. Además de las ventajas de esta separación, puede ser más fácil mantener los archivos organizados de esta manera. Una forma de organizarlos podría ser de acuerdo a los niveles de acceso establecidos por los mecanismos de control.

Varias compañías han desarrollado control de acceso a los sistemas utilizando variedad de hardware y software. Los paquetes proveen de tres características básicas: Autenticación del usuario, generalmente a través de verificación de password, acceso limitado a archivos (solamente lectura o sólo ejecución) o sin acceso, un registro de auditoría que es un reporte de quien acceso que archivos y cuando lo hizo.

Algunas características adicionales para los sistemas incluyen:

- *Encriptación transparente.* Este mecanismo puede ser útil si un usuario obtiene el acceso al sistema operativo, a través de programación, o a través de respaldos en línea de archivos, provocando la salida de un programa en ejecución o a través de una falla en el sistema de seguridad. Algunos sistemas automáticamente encriptan los archivos del sistema operativo por lo que aunque sean accesibles su contenido no es evidente.

- *Tiempo de acceso.* El administrador de seguridad puede implementar permisos para que los usuarios accesen el equipo sólo durante determinadas horas, y sólo durante determinados días de la semana. Este control asegura que los empleados o intrusos no pueden merodear los sistemas después de las horas de oficina para tratar de penetrar en los sistemas. Aunque esto también tiene sus contrapuntos ya que muchas personas se quedan a trabajar después de su horario para terminar sus labores o hacer trabajos urgentes.

- *Cierre automático del sistema.* Con este tipo de control activado, el

- sistema termina la sesión de un usuario, que no teclea algo durante determinado tiempo. El sistema pone una protección de pantalla y necesita de una nueva Autenticación para ser reiniciado. Lo que elimina la amenaza de un interceptor que vaya pasando.

- *Identificación de máquina.* Un sistema puede utilizar mecanismos de hardware que responda con un único número serial que puede ser leído por una aplicación de software. Cada mecanismo de hardware identifica una sólo máquina, evitando el robo de componentes.

Seguridad en Sistemas Unix

Los sistemas Unix son los sistemas multiusuarios más prevalecientes y también los servidores en Internet más comunes. Por lo que es conveniente considerar las características del manejo y administración de estos sistemas.

Los sistemas Unix son muy poco intuitivos, sus comandos y sintaxis lleva a la gente que no esta familiarizada con el sistema a cometer error tras error, que resulta en ocasiones desesperante, especialmente cuando se esta acostumbrado a los ambientes gráficos bastante amigables. Algunos archivos de configuración son listas de acciones que deberán ser ejecutadas por el sistema. Los administradores de estos equipos no se pueden dar el lujo de poner un carácter en lugar de otro, ya que su efecto podría ser desastroso en cualquier configuración.

El resumen que presentamos es un breve esbozo del sistema Unix, y lo que a nuestra consideración cualquier administrador de este sistema debe tener en mente:

Mantener las Instalaciones de Software Actualizadas

Los sistemas Unix están en un cambio constante. En algunos casos, el cambio es para añadir nuevas características y en otra para arreglar problemas de versiones anteriores.

Manejo de Cuentas de una Forma Adecuada

Un segundo problema en la administración de cualquier sistema es mantener las cuentas actuales. Un usuario siempre estará pidiendo por una nueva cuenta, generalmente mientras haya espacio no habrá problemas para crearla, pero el administrador siempre tendrá problemas para borrarla, por que no se entera cuando el empleado sale de la empresa o ya no la usa.

Cuentas sin Usar

Las cuentas que no se han utilizado por mucho tiempo, a alguien que esta fuera de esta por un período largo, o pueden corresponder a usuarios que se cambiaron de servidores pero conservan su cuenta en el servidores anterior. Muchos intrusos buscan cuentas con poco uso para realizar sus ataques desde ahí.

Cuentas Expiradas

Los usuarios que dejan la empresa, suelen representar un serio problema, si este usuario dejo la empresa en no muy buenos términos, puede ser que quiera accesar el sistema para causar algún tipo de daño. Para esto debe existir una línea de comunicación entre la oficina de recursos humanos y el administrador de los sistemas para que cuando la persona abandone la empresa se le cancelen sus cuentas.

Cuentas de Invitados

Algunos sistemas tienen cuentas para invitados o cuentas demo; o son instaladas para permitir el almacenar archivos en algún servidor. Este tipo de cuentas deben ser eliminadas, y si alguien llega a requerir algo parecido, lo mejor es crear cuentas con tiempo de expiración y privilegios restringidos para estos individuos conforme lo vayan necesitando y cerrarlas tan pronto ya no se requieran.

Cuentas Anónimas

Suelen ser utilizadas para permitir acceso a la gente externa, para recuperar archivos públicos. Estas cuentas deben establecerse de forma muy cautelosa, incluso lo mejor es dedicar una máquina completa para este tipo de información y no conectarla a otro tipo de máquinas, que contengan información más sensible.

Mantener una Autenticación de Usuarios Estricta

Un acercamiento muy prudente es el limitar a los programas para que sólo accesen los recursos que necesitan. Es muy conveniente también el dar a los usuarios los privilegios más elementales para que realicen sus tareas.

Los archivos que contienen los passwords de las cuentas de Unix, tienen muchas cosa información poco relacionada con la Autenticación de los usuarios. Es conveniente, por ejemplo, el separar la información (nombres de los usuarios y otros datos administrativos) y la que debe ser la más protegida (los passwords encriptados). Muchos programas necesitan accesar la parte pública, pero sólo algunos programas, aquellos que trabajan la Autenticación y el manejo de passwords, requieren acceso a el archivo de passwords encriptados, pensando en lo que podría pasar si alguien tuviera acceso a este archivo, lo mejor seria no darle muchos privilegios, por ejemplo, el darle a la rutina de Autenticación acceso de lectura general es un privilegio excesivo. Una mejor solución es crear un grupo que tenga acceso al archivo de password encriptados y que la rutina de Autenticación pertenezca a ese grupo. De esta manera si un intruso, que penetra la rutina de Autenticación, sólo podrá tener acceso al archivo de password, y no a todos los archivos sensibles.

Auditoría

Los administradores deberían utilizar las facilidades dadas por los sistemas Unix para desarrollar su propia herramienta para hacer el análisis de auditoría de forma automática. También deberían de tener el hábito de monitorear las actividades del sistema (usuarios, tiempo de acceso, longitud de la sesión, procesos corriendo- varias veces al día, en forma aleatoria. Aunque esto no garantiza encontrar una agresión al sistema, el administrador deberá revisar los registros de auditoría para encontrar anomalías, y deberá utilizar herramientas automatizadas para encontrar inconsistencias.

Para la seguridad de los registros de auditoría, estos tendrán que ser enviados a máquinas diferentes a la que se le realizo la auditoría o mandar a imprimir los registros (nunca a un archivo en la misma máquina). Porque una de las primeras cosas que un agresor intentara hacer es, tratar de deshabilitar la auditoría, para evitar ser sorprendido.

Passwords

A pesar de los estudios que han demostrado que la elección de los passwords se hace en una forma bastante obvia y esto ha ocasionado muchas intrusiones como la de los incidentes de los gusanos de Internet, los cuales han tenido éxito en parte al pobre manejo de passwords, la seguridad de los passwords en sistemas Unix continua siendo una gran debilidad.

Muchos usuarios no eligen passwords difíciles de adivinar. Lo que el administrador del sistema podría hacer es:

- Educar a los usuarios sobre la importancia del password y su elección para el y todo el sistema
- Periódicamente revisar el archivo de passwords encriptados para buscar palabras comunes y hacerles alguna variación con el nombre del usuario.
- Ejemplificar como se podría acceder a una cuenta con un password que resulte obvio.

En el tercer capítulo continuaremos hablando de passwords.

Manejo de Seguridad en Redes

En esta parte se considera el manejo de la seguridad en redes. Como en las secciones anteriores, este tema no es tratado a profundidad sino de una manera muy general con los aspectos más relevantes.

- Distancia y Tamaño. Tanto la distancia como el tamaño no son problemas por si mismos, ya que es muy viable implementar una red segura que tiene nodos en varios continentes. Un ejemplo de esto son las redes militares o las corporaciones multinacionales.

  De cualquier manera la distancia y el tamaño pueden afectar la seguridad si la red no es administrada en una manera clara y consistente. Si es necesario hacer un cambio por razones de seguridad, el mismo cambio debe implementarse a todos los sitios afectados. De manera similar, cada sitio debe implementar su propia versión de seguridad en una organización común, pero de tal manera que cada parte de la red se soporte una a otra cooperativamente.

- Intrusos y usuarios. Si se tiene una red local, que esta conectada a una red otra red, es conveniente definir el perimetro de la red local a través de una valla virtual que separe a los usuarios locales de los intrusos que serían los que están afuera de la valla. Presumiblemente cuando existen daños es porque la valla ha sido rota.

  Aunque esto no siempre resulta ser cierto, ya que veinte personas que trabajan juntas se conocen y confían unas en otras, y ninguno de ellos haría algo antisocial o que dañara a algún colega, no así en una organización de veinte mil esparcidas por todo el mundo, por lo que los daños también pueden provenir de personas internas a la organización.

- Responsabilidad y propiedad. Internet difiere de muchas redes organizacionales, en un aspecto: no tiene un propietario, o es administrada o controlada por ninguna autoridad. Esta situación es el respaldo de la forma en como evoluciono. El lado positivo ha sido el tremendo avance en la tecnología de red que se ha logrado en un período tan relativamente corto. El lado negativo ha sido que si se desea expandir o cambiar alguna configuración son imposibles, por la anarquía que existe.

- La seguridad en Internet es muy irregular. Algunos sitios tienen una seguridad muy sólida, que depende de la fortaleza de su instalación y de su conexión con Internet para sus negocios diarios. Otros sitios son solamente proveedores de servido que le venden el acceso a cualquiera que lo solicite.

  En consecuencia, cada servidores conectado a Internet es un riesgo a parte. Razón para que cada administrador de servidores implemente sus medidas de seguridad para defenderse de cualquier ataque.

Arquitectura de las Redes

En orden de defenderse en contra del exterior, el administrador de red debe tener bien claro que esta protegiendo y de quien lo esta protegiendo. Puede ser que suene demasiado obvio, pero algunos administradores no conocen específicamente que recursos control y como están organizados. Tampoco saben que direcciones corresponden a que máquina y que máquinas son visibles desde el exterior.

Posiblemente el administrador no sea culpable, algunos administradores heredan

Una topología de administraciones anteriores, otros trabajan en un ambiente de configuración dinámica, en donde la gente puede añadir, quitar o reconfigurar equipo sin informarle al administrador. Finalmente, el bajo precio de los equipos y la tendencia hacia un fácil uso del software hace muy difícil aun para el mejor administrador mantener una visión actual de la configuración.

- *Conectividad.* Es difícil mantener un registro de la localización de las máquinas físicas, y puede ser más difícil mantener el registro de como están conectadas dichas máquinas. Las conexiones de afuera son, la mayor preocupación. Un ataque es un sólo evento, pero se deriva de una serie de debilidades. Por esta razón, es importante atender la seguridad de todas las máquinas de la organización. Una máquina ignorada, y pobremente administrada en una esquina es un buen objetivo para que los intrusos la utilicen de plataforma y entrar a todo el sistema. Un mapa de conexiones físicas es esencial. Trazando que máquinas pueden pasar procesos a otras máquinas.

- *Permisos.* Una vez que todas las máquinas y todas las conexiones son conocidas, el siguiente paso es desarollar un ambiente seguro para verificar permisos ente máquinas conectadas. Por conveniencia, los usuarios de una organización quieren tener acceso a los datos en todas las máquinas a las cuales tienen acceso. El medio más fácil para los usuarios es tener cuentas en todas las máquinas. De cualquier manera, el administrador debe continuamente monitorear los permisos en estos archivos para estar seguro que sólo las conexiones necesarias son permitidas. Aun cuando las condiciones fueron establecidas, algunos usuarios pudieron haberlas cambiado.

- *Respaldos.* Los respaldos de datos y aplicaciones son necesarios de tal forma que pueden ser recuperados en caso de una emergencia, pero el administrador de un sistema también debería mantener respaldos de toda la configuración del sistema. Preferentemente, estos respaldos deberían almacenarse en medios de almacenamiento diferentes. De esta forma si el sistema resulta dañado, el administrador puede saber que el respaldo no ha sido dañado. y recuperar seguramente el sistema de la copia sin tener que reconstruir el sistema.

Seguridad de los Servidores

Seguridad en la red, requiere de conexiones y asegurar cada conexión a un servidores, como se vio anteriormente, una máquina sin utilizar se puede convertir en plataforma para un ataque.

Versiones de Software

El software, como la mayoría de los elementos de cómputo. En algunos casos, la evolución trae nuevas características o funcionalidad, en otros caso actualiza el software para manejar nuevas situaciones, tal como nuevos mecanismos o funciones que reparan o descubren fisuras.

Cuentas

Algunos sistemas son enviados con una cuenta demostración, cuenta de invitado o cuenta de inicio para que el nuevo usuario, empiecen a utilizar el sistema rápido y fácil. Es necesario que están cuentas se borren. También existen sistemas que llegan con una cuenta de mantenimiento o para diagnostico remoto y servicio.

Justificación de Cuentas

Cada vez que un sistema este listo para ponerse en producción, y especialmente cuando va a ser conectada a una red accesible, cada cuenta que se cree deberá ser justificada y protegida por un estricto password.

Incidentes

A veces a pesar de que un sistema este bien administrado, algunas veces ocurren incidentes. Es mejor planear por adelantado los posibles incidentes y la mejor forma de solucionarlos.

Cada administrador de un sistema deberá desarrollar un plan de manejo de incidentes. El plan deberá contemplar las diferentes características:

- Los usuarios deberán reconocer comportamientos sospechosos del sistema y a quien reportárselos.

- El administrador del sistema deberá tener una lista de contactos de soporte técnico, a los que deberá acudir ante cualquier eventualidad del sistema.

- Según el tipo de incidentes, se deberán tomar determinadas acciones, como: cerrar operaciones, desconectarse de la red, monitorear las máquinas.

- Un medio por el cual poder notificar a los usuarios que el sistema ha sido afectado, y las acciones que deben ser tomadas.

Adicionalmente, cada administrador de un sistema deberá tener las herramientas, programas y datos necesarios para reconstruir el sistema lo más rápido y eficientemente posible. Respaldos periódicos deben ser hechos y guardados en un lugar seguro.

Herramientas de Ataque

Los atacantes han desarrollado herramientas para detectar debilidades en los Servidores, tales como cuentas sin passwords, cuentas con passwords triviales , configuraciones de permisos que permitirían a un intruso sobreescribir archivos de configuración importantes. El atacante utilizara estas herramientas en cualquier servidores accesible para determinara si un ataque puede o no ser perpetrado. Pero también existen muchas herramientas que sirven a los administradores para defenderse de estos ataques.

Algunas herramientas son:

- *CRACK.* Colección de herramientas verificadoras de passwords. Lo que hace es utilizar una lista de palabras comunes, para identificar las cuentas que tienen passwords que pueden ser identificados fácilmente. Trabaja en sistemas Unix que almacenan passwords de forma encriptada en Unix estándar.

- *Tripwire.* Es una herramienta que se utiliza después de una penetración sospechosa. En los sistemas grandes, muchos archivos pueden ser modificados en un período muy corto, pero, existen algunos, como los sistemas operativos y archivos de configuración, que están en binario, que no deben ser cambiados. El Tripwire es un verificador integral de archivos que compara las versiones activas de los archivos con las de respaldo para determinar que archivos han sido modificados.

- *COPAS.* Es un conjunto de programas que verifican archivos importantes del sistema, configuraciones de los usuarios y configuraciones de permisos; para descubrir fisuras o debilidades que pudieran ayudar a los atacantes. Generalmente esta herramienta por los administradores del sistema para probar la seguridad dentro de sus redes.

- *SATAN.* Colección de herramientas de análisis de red. SATAN, si trabaja afuera de las redes, no como COPAS, para verificar fisuras visibles. SATAN es un poco controversial, porque si tanto puede ser utilizado por administradores como atacantes.

Existen algunos argumentos por los cuales no es muy aceptado el hacer un análisis de riesgo, a pesar de que tiene herramientas que pueden ser utilizadas por auditores, contadores y administradores.

Los argumentos en contra que se tienen son los siguientes:

- *No es preciso.* La falta de precisión, continuamente es citada como una deficiencia. Los valores que se utilizan en el método, como es la probabilidad de ocurrencia y el costo por ocurrencia no son precisos.

  El análisis de riesgos es más una herramienta de planeación. Cuando es utilizada en esta forma, muestra cuales son las amenazas a las que es sometido el sistema y cuales pueden ser las más dañinas y deben ser tomadas en cuenta para un análisis costo-beneficio.

- *Falso sentido de precisión.* Otro argumento es que los números de pérdida tiene un falsa precisión de seguridad. Aunque es importante el tamaño de los número no es tan importante cuando se habla de daños importantes. Poner demasiada importancia en los números es una falla del usuario, no del método.

- *Inmutabilidad.* Análisis de riesgo, como los planes de contingencia y los planes a 5 años, tienen una tendencia a ser olvidados rápidamente. De cualquier forma, es tentador aceptar los resultados el año anterior, en lugar de tener que analizar y justificarlos cada año.

Algo importante a considerarse en la revisión anual, es ver que condiciones han cambiado y cuales siguen vigentes. También es importante no ser muy

dependiente del plan viejo, pero tomar cada oportunidad de revisión como una oportunidad para replantear y quizá corregir las prioridades estimadas basadas en la nueva experiencia. De esta manera, los valores del plan se vuelven más precisos cada vez que un nuevo análisis es hecho.

El argumento final en contra del análisis de riesgo es que no depende en teorías científicas, ni en principios científicos. Pero tampoco es cierto, El análisis de riesgo depende en principios de teoría de probabilidad y análisis estadístico.

CAPITULO III

Encriptación y Protocolos

El capítulo tres está dedicado a la encriptación y protocolos de comunicación para el manejo de comunicaciones seguras.

Este capítulo lo empiezo describiendo como funcionan las redes, que es el medio por donde viaja la información; describo lo que es la encriptación, sus orígenes, los algoritmos más conocidos y término hablando de protocolos y certificados de autenticación.

3. 1 Redes

En el capítulo anterior, hice mención a algunos aspectos de la seguridad en las redes, aquí retomo el tema, pero bajo una perspectiva diferente. Mientras más comunicación haya entre computadoras mayores vulnerabilidades encontraremos. Dentro de este mundo de comunicaciones existen tres tipos básicos de redes de cómputo, cada uno con características y riesgos propios:

Red de Área Local (LAN)

Son redes diseñadas para conectar computadoras que se localizan en la misma área geográfica y que pertenecen a un mismo dominio administrativo. Estas redes se encuentran típicamente en pequeñas organizaciones donde los empleados comparten recursos de cómputo -tanto servicios de hardware como impresoras y servicios de software como aplicaciones- y también tienen la necesidad de comunicarse una con otra. Una LAN típica esta limitada por lo general por un edificio, e incluye servicios de correo electrónico, transferencia de archivos, respaldo y recuperación de archivos. Cada máquina conectada a una red LAN debe tener software especial que le permita comunicarse con las otras máquinas del sistema.

Los crímenes perpetrados en una LAN generalmente son por empleados o personas con acceso a las instalaciones físicas donde se localizan las máquinas de esta red.

Las LAN son más vulnerables a un ataque foráneo cuando tienen gateways a otras redes, ya sean regionales, nacionales o corporativas (del tipo WAN que trataremos más adelante).

Red de Área Amplia

Son redes que cubren un área geográfica más grande de una ciudad o un área metropolitana. Las computadoras en una WAN están conectadas por circuitos de datos de larga distancia, de alta velocidad o arrendados. Cuando las WAN son relativamente pequeñas en tamaño (a veces llamadas MAN Metropolitan Area Networks, Redes de Área Metropolitana) y generalmente se conectan vía cable coaxial, microondas o fibra óptica.

Internetworks

Las redes pueden ligarse unas a otras para permitir a los usuarios en una red el comunicarse con otros usuarios. Un método común para conectar redes es por medio de un gateway (que es un sistema que forma parte de dos o más redes). De esta forma la información pasa de una red a otra a través del gateway que esta conectada a ambas redes.

Internet (en el capitulo 4 ahondo más sobre este tema) es la red interconectada más grande en el mundo que esta en operación, esta compuesta por miles de WAN y LAN interconectadas. Esta red tiene alrededor de 120 países conectados en los 7 continentes con 2 000 000 servidores conectados y varios millones de usuarios, y su crecimiento se duplica aproximadamente cada 9 o 10 meses. Este crecimiento ha traído cambios tecnológicos y legislativos (de lo cual hablamos en el primer capítulo).

Comunicación entre Redes

Cuando se envía un mensaje de una computadora a otra que se encuentran físicamente a miles o millones de kilómetros, este mensaje viaja a través de varias computadoras por medio de una serie de redes conectadas, que se utilizan como recipientes. Y al pasar por cada una de estas computadoras, los mensajes se van haciendo más vulnerables.

Existen dos tipos de transmisión de datos: analógica y digital. Las redes de transmisión de voz típicamente usan circuitos analógicos capaces de transmitir un rango de sonidos. Los circuitos de comunicaciones digitales utilizan el principio binario para transmitir información en una forma digital. Debido a que la comunicación entre computadoras utilizan circuitos digitales, pero sus comunicaciones son llevas a través de canales análogos, módems (modulator-demodulator) que se necesitan para ejecutar la conversión necesaria. Un módem

convierte la información digital de una computadora a información analógica para poder ser transmitida. Cuando la información es recibida, se utiliza otro módem para reconvertir la información, esta vez a un formato digital para que pueda ser interpretada por la computadora.

Existen varias formas para proteger las comunicaciones, incluyendo control de acceso, métodos criptográficos, tecnología firewall y otras medidas físicas (como protección del cableado de red).

Passwords

El control de acceso es crucial para reforzar la seguridad de cómputo en un ambiente de red, la razón por la que hago tanto hincapié en este tema es porque ésta es una de las formas más utilizadas de seguridad y no es todo lo eficiente que debiera. Muchos sistemas usan passwords como medios de control de acceso. Por eso es importante que el password no sea conocido más que por la persona que es dueña de la cuenta o el servicio de cómputo que es protegida por el password.

Algunas reglas básicas para el cuidado de passwords:

- Nunca escribir el password y dejarlo cerca de la computadora
- Nunca crear passwords que utilicen el nombre del usuario o alguno otro que sea fácil de adivinar
- Nunca compartir el password con nadie
- No almacenar passwords en la computadora

Aunque la mayoría de las organizaciones dejan a los usuarios elegir sus passwords, otras prefieren adicionar controles a esta elección como:

Tipo de Password	Descripción
Passwords generados por el sistema.	Algunos sistemas le dan a los usuarios passwords generados de forma aleatoria, y aunque el sistema se asegura que los passwords sean pronunciables, generalmente son difíciles de pronunciar. Desafortunadamente, esto causa que muchos usuarios tengan que escribirlos, con lo que rompen con el propósito principal.

Longitud de password.	Los passwords de longitud grande son más seguros que los de longitud corta, porque son más difíciles de adivinar y toma más tiempo penetrarlos. Muchos sistemas imponen una longitud mínima en los passwords.
Expiración de passwords	También se usa que los usuarios tengan que cambiar su password cada determinado tiempo
Limite de intentos de conexión	Muchos sistema tienen un numero de veces limite para que los usuarios traten de conectarse
Mensaje de ultima conexión.	Cuando los usuarios se conectan, algunos sistemas despliegan la hora de la ultima vez que el usuario estuvo conectado.
Archivos encriptados.	Muchos sistemas encriptan los archivos que contienen los passwords y mantienen estos passwords en lugares seguros dentro del sistema, disponibles sólo para los administradores del sistema y el mismo sistema de passwords.
Seguros de passwords.	Los administradores del sistema pueden utilizar seguros para restringir a ciertos usuarios accesar ciertos sistemas, o restringir usuarios a ciertos equipos, o bloquear las cuentas excepto durante determinadas horas de trabajo.
Passwords adicionales.	Para determinados sistemas puede ser necesario introducir el password del sistema y el password del usuario. Un segundo password puede ser requerido para acceso por módem. En algunos sistemas altamente sensitivos, puede requerirse que dos usuarios introduzcan su password antes de que el sistema les permita entrar.
Tarjetas Inteligentes.	Algunos sistemas para permitir el acceso a los usuarios pueden requerir vía tarjetas inteligentes que necesitan el uso numero de identificación personal (PIN), antes de permitirles el acceso.
Passwords no reusables	Passwords que se utilizan una sola vez. Debido a que estos passwords no se almacenan en ningún lado para uso posterior, son difíciles de robar. El método es utilizar un algoritmo de encriptación, que consiste en generar una serie de secuencias de registro (quizá 20 a la vez), que codifica una palabra corta. Que puede ser impresa y cargada por el usuario. La primera vez que el usuario se conecta utiliza la primer palabra; la segunda vez, utiliza la segunda palabra....
Passwords basados en tiempo.	Con ciertos tipos de sistemas de autenticación, los passwords varían cada minuto. Una tarjeta

	inteligente despliega alguna función de la hora actual y la clave secreta del usuario. Para obtener el acceso, el usuario debe introducir un número basado en su clave y la hora actual.

Protección del cableado de red

Para reforzar la seguridad de las comunicaciones, algunas veces se requiere de medidas físicas. Los cables que llevan la información son muy vulnerables a los intrusos. Un atacante puede deshabilitar toda una sección de la red simplemente cortando el cable de comunicación. La fibra óptica es más difícil de cortar y también de reparar. Un método de protección simple, aunque caro es poner el cable de red entre de conductos de acero. Algunas instalaciones de alta seguridad utilizan paredes dobles de seguridad con gas a presión entre las capas, si la presión baja como consecuencia de la rotura de alguna capa, una alarma es encendida.

Escudos

Una frecuencia de radios utilizado como escudo puede evitar la intercepción de emisiones electromagnéticas. Típicamente, un escudo, atenúa las señales conduciéndolas a tierra, antes de que puedan escapar. Los escudos pueden proteger computadoras, cables o edificios enteros.

Tecnología Firewall

Una forma efectiva de proteger un lugar de atacantes mientras se le permite a los usuarios el accesar los servicios de Internet es construyendo un firewall. Para que sea efectivo, un firewall, debe ser configurado, instalado y mantenido con gran cuidado.

Un firewall es un acercamiento hardware/software que restringe el acceso forzando todas las comunicaciones de red - aquellas que viajen de redes internas a Internet y aquellas que viajan de Internet a redes externas- pasen a través del firewall. Un firewall también puede proteger una parte de la red interna del resta de la red.

Las organizaciones pueden organizar sus firewalls en una gran variedad de formas. Algunos lugares pueden utilizar un firewall para bloquear completamente todo acceso a y desde Internet. Otros pueden limitar el acceso a una máquina en particular o los usuarios pueden conectarse vía Internet a máquinas fuera de la red interna. Algunos pueden reforzar reglas más elaboradas para examinar cada mensaje o comunicación que pase de fuera hacia a adentro o viceversa, para asegurarse que se está cumpliendo con la políticas de seguridad.

3.2 Encriptación

La encriptación es la ciencia que permite la transmisión segura de información a través de la transformación de los datos en forma reversible.

La encriptación es el proceso de codificación de la información de tal manera que no pueda ser fácilmente descifrada sin el uso de mecanismos o procedimientos de desencriptación (proceso inverso), o sea la transformación de información encriptada a su formato original.

La encriptación se toma en muchas ocasiones como sinónimo de seguridad, debido a que las rutinas de encriptación fueron utilizadas mucho tiempo antes que existieran acercamientos de detección, controles de acceso o algún otro tipo de protección. Por lo que muchos individuos han utilizado la encriptación como el medio principal para proteger su información y recursos.

Uno de los motivos que originó la necesidad de crear mecanismos o métodos para encriptar información fue el lograr que información relevante se mantuviera protegida y que sólo pudiera ser leída por aquellos a los que iban dirigida o por el dueño original. Para lograr esto se inventó una gran variedad de formas para convertir un texto legible a una forma de texto encriptado, y que a partir de éste último, y en ocasiones con alguna otra información, permitiera recuperar el texto original (texto plano). Sin embargo, lo que no es muy reconocido es que muchas rutinas de encriptación son fácilmente rotas con sólo un poco de paciencia y esfuerzo por parte de los intrusos. Lo que mina en cierta forma la confiabilidad de este mecanismo, otro problema reside en que si la persona para desencriptar la información no tiene las rutinas de desencriptación, la información encriptada puede ser pérdida.

Como resultado de esto, se han planteado algunos mecanismos para optimar el rol de la encriptación enfocándolo a la protección de información. En particular, la importancia de la encriptación reside en que es un a forma para establecer una Autenticación distribuida y como una mediada para evitar amenazas a los datos que se transmiten.

Uno de los métodos de encriptación más utilizados es uso de las llaves para encriptar la información, las llaves se clasifican en privada y pública. La llave privada, también llamada llave simétrica o llave secreta, utiliza la misma llave tanto para encriptar como para desencriptar datos. Con la llave de encriptación pública, debe existir dos llaves relacionadas con un mismo mensaje encriptado, el mensaje se encripta con una llave pública que puede ser desencriptada solamente con su correspondiente llave privada. Antes de seguir desarrollando los métodos más eficientes de encriptación, presento un cuadro del papel de la encriptación en el tiempo:

Antecedentes Históricos

Realizar una reseña histórica exhaustiva de la encriptación podría ser en mismo un trabajo de investigación y muy extenso, por esta razón considero que hacerlo me distanciaría del objeto de estudio que propongo realizar, por lo que me limitaré únicamente a dar una lista de los eventos más sobresalientes. No sin mencionar que son muchos los caminos que se han seguido para llegar a lo que hoy conocemos como seguridad en cómputo y encriptación.

A continuación en listo los acontecimiento históricos más sobresalientes:

Fecha	Acontecimiento
1900 a.C.	Un escriba egipcio utilizó escritura jeroglífica no estándar en una inscripción (KAHAN 1967).
1500 a.C.	Una tabla mesopotámica contenía una fórmula encriptada para hacer artículos de alfarería. (KAHAN 1967).
500-600 a.C.	Los escribas hebreos escribían anotaciones encriptadas en el libro de Jeremías usando un alfabeto invertido (substitución simple) y esta técnica de encriptamiento es conocido como ATBASH.
487 a.C.	Los griegos utilizaban un mecanismo llamado skytale - formado de una estaca en la que se enrollaba una tira de cuero sobre la que se escribía y luego era usado como cinturones). Para poder desencriptar el mensaje se requería tener otra estaca de las mismas dimensiones (KAHN 1967).

50-60 a.C.	Julio Cesar usaba sustitución simple con el alfabeto normal, en el que únicamente se hacía un corrimiento en el orden de los caracteres (p. ej. el corrimiento podría ser 5, en el caso de la 'a' se utilizaría la 'f'). Este sistema era más débil que el ATBASH (KAHAN 1967).
? d.C.	El Kama Sutra en el 44to. y 45to. artes (yoga) hace referencias a la encriptación. • 44to. El arte de entender escritura encriptada, y escribir palabras en forma peculiar. • 45to. El arte de hablar cambiando la forma de las palabras, algunos hablan cambiando el inicio y final de una palabra, otros agregando letras innecesarias entre las sílabas de una palabra, etc. (BURTON 1991).
200 a.C.	Los llamados papiros de Leiden empleaban encriptadores para ocultar partes importantes de recetas mágicas (KAHAN 1967).
725-790? d.C.	**Abu 'Abd al Rahman al-Khalil ibn 'Amr ibn Tammam al Farahidi al-Zadi al Yahmadi** escribió un libro de encriptación, inspirado en la solución hecha por el mismo al criptograma escrito en griego del emperador Bizancio. Su solución estuvo basada el conocimiento del texto no cifrado al inicio del mensaje (este es un método estándar y que se uso en la Segunda Guerra Mundial contra los mensajes de ENIGMA). (KAHAN 1967).
855 d.C.	**Abu Bakr Ahman ben 'Ali ben Wahsiyya an-Nabati** publicó varios alfabetos para encriptamiento que eran usados en la magia. (KAHAN 1967)
1226 d.C.	A inicios de 1226 aparece una política de encriptación no muy bien definida en los archivos de Venecia, en la que puntos o cruces sustituían las vocales en algunas palabras. (KAHAN 1967).
1379 d.C	Gabrieli di Lavinde a petición de Clemente VII compiló una combinación de un alfabeto de sustitución y un código pequeño. - Esta clase de código/encriptación fue utilizado por diplomáticos y civiles por los siguientes 450 años a pesar de que fueron inventados métodos de encriptación más fuertes durante ese tiempo
1392 d.C.	"The Equatorie of the Planets", posiblemente escrito por Geoffrey Chaucer, contiene pasajes encriptados. El método de encriptación es una simple sustitución mediante un alfabeto formado de letras, dígitos y símbolos
1466 d.C.	Leon Battista Alberti inventó y publicó el primer polialfabeto de encriptación, diseño un disco de encriptación para simplificar el proceso. No fue roto hasta el siglo XIX. Alberti también escribió

	sobre el arte del encriptamiento.
1473-1490 d.C.	Un manuscrito de Arnaldus de Bruxella usa cinco líneas encriptadas para ocultar la parte medular de la operación para hacer la piedra filosofal.
1518 d.C.	Johannes Trihemius escribió el primer libro impreso sobre criptología. Inventó un encriptador en el que cada letra representaba una palabra tomada de una sucesión de columnas. La serie de palabras resultantes podían ser oración legítima. También escribió un encriptador polialfabético de sustitución. Introdujo la noción de cambio de alfabeto en cada letra.
1553 d.C.	Giovan Batista Belaso introdujo el uso de una palabra clave como llave de un encriptador polialfabético de repetición.
1563 d.C.	Giovanni Battista Porta escribió un texto sobre encritptadores e introdujo el encriptador diagráfico. Clasificó a los métodos de encriptación como transposición, sustitución y sustitución de símbolos. Sugirió el uso de sinónimos y errores ortográficos para confundir a los criptoanalistas. Aparentemente introdujo el concepto de alfabeto mixto en tablas polialfabéticas.
1585 d.C.	Blaise de Vigenere escribió un libro sobre encriptación, que incluía el primer sistema de autollave para encriptar texto (la idea del autollave se encuentra presente en el DES).
1790 d.C.	Thomas Jefferson, posiblemente ayudado por el Dr. Robert Patterson (un matemático de la Universidad de Pensilvania.), inventó la rueda encriptadora. Está fue reinventada de muchas maneras y usada en la segunda guerra mundial por la armada de los E.U. (M-138-A).
1817 d.C.	Decius Wadworth produjo un disco de encriptación engranado con números y letras y alfabetos encriptados.
1857 d.C.	Sir Francis Beaufort creó un encriptador conocido como Vigenere y fue públicado por su hermano después de su muerte.
1859 d.C.	Pliny Earle Chase publicó la primera descripción de un encriptador fraccionario.
1861 d.C.	Friedrich W. Kasiski publicó un libro en el que da la primera solución general a un encriptador polialfabético con palabra clave lo que marco el final de cientos de años de los alfabetos polialfabéticos fuertes.

1861 d.C.	Durante la guerra civil de E.U. se utilizaban encriptaciones de transposición y el encriptador Vigenere.
1891 d.C.	Etienne Bazeries hizo su versión de la rueda encriptadora y publicó su diseño en 1901 después de que la armada Francesa lo rechazó.
1913 d.C.	Parket Hitt reinventó la rueda encriptadora en forma de tiras (strip cipher), dando origen al método M-138-A de la segunda guerra mundial.
1917 d.C.	William Federick Friedman fue honrado como el padre del criptoanálisis de E.U. (acuño el término criptoanálisis). Fue empleado como criptoanalista en los laboratorios Riverbank. Trabajó para el gobierno de E.U. ya que este no contaba con criptoanalistas expertos
1917 d.C	Gilbert S. Vernam trabajo para AT&T e inventó una máquina cifradora polialfabética capaz de usar llaves completamente aleatorias, que nunca se repetían. Esta máquina fue ofrecida al gobierno de E.U. para ser usada en la primera guerra mundial pero no fue aceptada y se comercializó en 1920
1917 d.C.	El sistema ADGVX fue puesto en servicio por los alemanes a fines de la primera guerra mundial. Este sistema utilizaba sustitución a través de un arreglo de llaves, fraccionamientos y transposición y fue roto por el criptoanalista francés Georges Painvin
1919 d.C.	Hugo Alexander Koch patentó en Holanda una máquina de encriptación basada en un rotor. Esta máquina impulsó a una familia de máquinas de encriptación bajo la dirección de Boris Caesar Wilhelm Hagelin, quién se introdujo en el negocio y comercialización de encriptación. Después de la guerra una ley sueca autorizó al gobierno para apropiarse de estos inventos lo que obligó a Hagelin mover su compañía a Suiza donde fue incorporada como Crypto A.G. Esta compañía aún funciona.
1921 d.C.	Edward Hugh crea la "Herben Electric Code". Una compañía constructora de máquinas de encriptación electromecánicas basadas en rotores giratorios.
1923 d.C	Arthur Scherbius crea una compañía para construcción y venta de la máquina Enigma.
1924 d.C	Alexander Von Kryha produjo su máquina codificadora y que a pesar de ser criptográficamente débil, fue usada incluso por los cuerpos diplomáticos Alemanes (1950s). Esta máquina fue sujeta a prueba y los criptoanalistas norteamericanos Friedman, Kullback, Rowlet y Sinkov, lograron desencriptar un criptograma de 1135 caracteres en 2 horas y 41 minutos

1933-45 d.C.	La máquina Enigma no fue un éxito comercial, sin embargo fue mejorada y se convirtió en la base criptográfica de la Alemania Nazi (fue descifrada por el matemático Polaco Marian Rejewski).
1970 d.C.	Dr. Horst Feistel dirigió un proyecto en los laboratorios Watson Researche de IBM, y a partir de éste se creó el DES y algunos otros productos de cifrado formando la familia Feistel.
1976 d.C.	Un diseño de IBM basado en el algoritmo de encriptación Lucifer fue escogido para ser "Data Encryption Standard". (DES). Desde entonces ha tenido una gran aceptación debido a que ha mostrado ser suficientemente fuerte durante veinte años.
1976 d.C.	Whitfield Diffie y Martin Hellman públicaron "New Directions in Cryptography" dónde introdujeron el concepto de encriptación de llave pública, así como la idea de autenticación mediante el poder de funciones unidireccionales.
1977 d.C.	Abrol de 1977, Ronald L Rivest. Adi Shamir y Leonard M. Adleman, siendo novatos en encriptación se inspiraron en el artículo de Diffie y Hellman, y una noche de abril, Rivest se levantó por un intenso dolor de cabeza y creo el algoritmo RSA. A la mañana siguiente lo hizo llegar a Shamir y Edellman. El algoritmo RSA es un encriptador de llave pública de uso práctico tanto para confidencialidad como firmas electrónicas basado en la dificultad de factorizar números muy grandes. Rivest, Shamir y Adleman enviaron ésta idea a Martin Gadner el 4 de abril para su públicación en el Scientific American, apareciendo en la revista de septiembre de 1977. El artículo ofrecía enviar un reporte técnico completo a cualquiera que enviara su dirección en un sobre con timbre. Hubo miles de solicitudes de todo el mundo. Shamir cree que esto originó la política de que reportes técnicos y artículos pueden ser distribuidos gratuitamente (las revistas "Cryptología" y "The Journal of Cryptology" fueron fundadas poco después del intento de NSA, national security agency, de restringir el acceso a públicaciones). El algoritmo RSA fue públicado en 1977 en "The Communications of The ACM".
1984 d.C.	El encriptador ROT 13 fue introducido en el software "USENET News" para permitir la encriptación de imágenes y textos que pudieran insultar a ojos inocentes. Este es el primer ejemplo encriptador conocido por cualquiera que ha demostrado ser efectivo.
1990 d.C.	Xuejia Lai y James Massey en Suiza públicaron "A Proposal for a New Block Encryption Standard", que era una propuesta del International Data Encryption Algorithm (IDEA) , para reemplazar al DES. Esta idea USA llaves de 128 bits y emplea operaciones propias de computadoras de propósito general, lo que hace la implementación de sofware más eficiente.

	• Phil Zimmerman liberó su primera versión del PGP (Pretty Good Privacy) como respuesta al intento del FBI de tener acceso a la comunicación de los ciudadanos. A pesar de que el PGP ofrece sólo un poco más de los productos que actualmente están disponibles como el Mailsafe de RSADSI, el PGP es notable porque fue liberado como software gratis y se ha convertido en un estándar en todo el mundo. • 1994. Ron Rivest autor de los algoritmos RC2 y RC4 incluidos en la librería de encriptación RSADS'S BSAFE publico la propuesta del algoritmo RC5 en Internet. Este algoritmo utiliza rotación dependiente de los datos como una operación no lineal y es parametrizado por lo que el usuario puede modificar el tamaño del bloque, el numero de vueltas y el tamaño de la llave.

Esas fueron las bases de la encriptación que hoy conocemos. Ahora voy a explicar algunos de los tipos de encriptación que existen y sus respectivos algoritmos.

3.2.1 Tipos de Encriptación

Algoritmos Impenetrables.

Para hacer que la información sea encriptada de tal manera que no pueda ser descifrada fácilmente por ningún intruso, se hizo necesario el utilizar algoritmos con fuertes bases matemáticas, algunos métodos para realizar la encriptación son la sustitución y la transposición y el uso de llaves.

Sustitución

El proceso de sustitución consiste en que cada carácter del texto original, será reemplazado con algún otro carácter. El resultado de la substitución, será un texto encriptado que no se parece al original de ninguna forma obvia. Quizá el ejemplo más famoso de sustitución es el de la sustitución Cesar (presumiblemente utilizada por los Romanos para encriptar mensajes) en el que un carácter del texto original es reemplazado por otro que se localiza a una distancia fija de ese carácter en el alfabeto. Esto puede ser visto como la clave para su encriptación y desencriptación.

Por ejemplo, si tenemos el texto "La criptografía es", en el que cada caracter va a ser sustituido por su equivalente en el alfabeto ASCII después de sumarle 11 posiciones tendremos que :

L	a	c	r	i	p	t	o	g	r	a	f	i	a	e	s
76	97	99	113	105	112	116	111	103	114	97	102	105	97	100	115

La sustitución seria:

87	108	110	124	125	123	127	122	114	125	108	113	115	108	111	126
W	l	n	{	}	l	Ç	z	r	}	l	q	s	l	o	Ç

Entonces el texto quedaría como:

Wln{}lÇzr}lqsloÇ

Transposición

La transposición consiste en una secuencia de caracteres del texto original, que se reacomodan en una secuencia diferente. El resultado de esta transposición será al igual que la sustitución un texto encriptado, que de ninguna forma recordara el texto original. Un ejemplo muy conocido de transposición es la matriz de transposición.

En esta matriz de transposición, un mensaje es visto como una matriz de NxM caracteres que pueden ser descifrados leyendo los renglones de la matriz de izquierda a derecha y de arriba hacia abajo.

Por ejemplo:

L a c r i
p t o g r
a f i a e
s e l p r

Si la matriz se interpretara de arriba hacia abajo el mensaje seria: Lpasatfecpilrgapirer, mensaje que no podría ser tan fácilmente interpretado.

Llaves

La utilización de llaves para codificar o decodificar información brinda flexibilidad y refuerza la protección a través de la autenticación. La llave se puede visualizar como información adicional necesaria para poder encriptar o desencriptar los datos.

Funciones Unidireccionales (ONE WAY FUNCTIONS)

Una función unidireccional es una función matemática que es fácil de calcular en una dirección y difícil de calcular en sentido contrario, por ejemplo una función de este tipo puede ser calculada en segundos pero calcular su inverso puede llevar meses o años.

Dentro de la encriptación existen unas funciones llamadas Trap-door "puertas falsas"; estas funciones son unidireccionales, y son fáciles de calcular en sentido inverso si se cuenta con alguna información, de lo contrario es sumamente difícil.

No se puede tener la seguridad de que una función de puerta falsa sea realmente complicada de calcular en sentido inverso, se cree en base a la experiencia que se requiere un gran esfuerzo para calcular en este sentido (fuerza bruta); pero no se puede asegurar que no exista algún método que facilite dicho cálculo, sin embargo, también en base a la experiencia se sabe que hasta ahora no ha sido fácil encontrar dichos métodos. Es por esto que este tipo de funciones son de mucha utilidad en encriptación.

En los sistemas de llave pública, las funciones unidireccionales son muy usadas para firmas digitales (muy útiles en los certificados), normalmente el tamaño de la llave corresponde a al tamaño de la entrada de la función (unidireccionales) y entre más grande sea la llave, se requiere un mayor esfuerzo para calcular a la función en sentido inverso. Por lo que en el caso de firmas digitales el tamaño de la llave nos dará mayor o menor grado de seguridad.

Es importante aclarar que el sentido que aquí se le da al hecho de que una función sea reversible, es desde el punto de vista computable, que difiere de que se tiene en matemáticas. Para establecer esta distinción daremos la definición de una función unidireccional:

Una función f es una función unidireccional si, para cualquier argumento x en el dominio de f, es fácil de computar el valor correspondiente ***y=f(x)****; sin embargo para cualquier* ***y*** *en el rango de* ***f****, es computablemente no factible, dado un valor de* ***y*** *y conociendo a* ***f*** *, calcular cualquier* ***x*** *aún no habiendo duda de que* ***f(x)=y****. Es importante hacer notar que una función que ha sido definida como no invertible desde el punto de vista computacional es completamente diferente al sentido que se le da normalmente en matemáticas. Una función* ***f*** *normalmente se conoce como no invertible cuando el inverso de un punto y no es único, por ejemplo, si existen puntos distintos* ***x1*** *y* ***x2*** *tal que* ***f(x2) = y = f(x2)*** *este no es el tipo de dificultad en la inversión de una función que nosotros requerimos en encriptación. En cambio, debe ser abrumadoramente difícil, dado un valor de* ***y*** *y conociendo a* ***f, calcular cualquier x,*** *aún no habiendo duda de que* ***f(x)=y***

Algoritmo de Encriptación

En el proceso de cifrado se requieren dos funciones, la primera para relacionar texto plano con texto cifrado y la segunda para realizar el proceso contrario. Cada transformación debe tener una operación inversa única, identificada por una llave criptográfica. Los tipos de algoritmos de encriptación, más importantes son el simétrico y el de llave pública.

Encriptación Simétrica

Este tipo de encriptación utiliza un sola llave simétrica para encriptar y desencriptar un archivo o mensaje. Por lo tanto, quien envía y quien recibe deben tener la misma llave y el mismo algoritmo de encriptación.

Para el uso seguro de una sola llave de encriptación se requiere cambiar constantemente y una transmisión segura de las llaves entre las partes intervinientes.

El algoritmo de negociación Diffie-Hellman produce una llave secreta en cualquier lado de la transacción, la cual nunca es enviada a través de la red. Esta llave es mezclada en alguna con el password, creando una llave de sesión maestra. Esta llave es utilizada para encriptar o desencriptar todo el tráfico de la conexión

Encriptación Asimétrica

Bajo este esquema, las llaves vienen en pareja. Una llave (la llave pública) se utiliza para codifica el mensaje, una segunda llave (la llave privada) se necesita para decodificar el mensaje. Por lo general, la encriptación asimétrica es muy utilizada para autentificar a un proveedor de servicio y establecer una sesión.

Los algoritmos de encriptación de llave pública utilizan una llave llamada pública para encriptar, y que es dada a conocer a todo el público, pero a diferencia de la llave de encriptación convencional se requiere de una llave distinta a la pública para el proceso de desencriptado, llamada llave privada.

Aparentemente la encriptación de llave pública es una opción que permite destacar a la encriptación simétrica, sin embargo hay algunos casos en los que es conveniente usar encriptación simétrica.

Una de las ventajas evidentes de la encriptación de llave pública es que nos proporciona un mayor grado de seguridad ya que no se requiere dar a conocer la llave privada, si alguien nos envía un texto encriptado con nuestra llave pública nosotros podremos obtener el texto plano mediante nuestra llave privada (que sólo nosotros conocemos). Si alguien nos envía un texto encriptado mediante una llave criptográfica también deberá enviarnos dicha lleve, lo que obviamente reduce el grado de seguridad; y que además es un problema por si mismo, ya que se debe de resolver el cómo hacer llegar dicha llave al destinatario.

Un problema que se presenta es el poder determinar si el que envia el mensaje es quien realmente dice ser. La encriptación de llave pública nos proporciona la facilidad de firmar electrónicamente - tema a tratar más adelante- los mensajes que encriptamos.

Finalmente cabe mencionar que existen algunos esquemas que usan los dos tipos de algoritmos de encriptación existentes. En el caso en el que se requiere encriptar rápidamente; los sistemas simétricos son mucho más rápidos que los de llave pública, por ejemplo, supongamos que queremos encriptar un texto plano muy grande y enviarlo a alguien, entonces lo mejor es utilizar un sistema simétrico.

A manera de historia, menciono que la encriptación pública nace ante la necesidad de resolver el problema de administración de llaves de la encriptación simétrica (¿Cómo hacer llegar al receptor de un mensaje la llave secreta sin correr el riesgo de que caiga en manos de alguien no autorizado?). El concepto de llave pública fue introducido en 1976 por Whitfield Diffie y Marti Hellman.

3.2.2 Encriptación de Verificación de Sumas (Checksumming)

Son funciones hash que toman como entrada los tamaños de las variables y regresan una cadena de un tamaño fijo. Los que se utilizan para la encriptación son unidireccionales(difíciles de invertir), y dan resultados únicos para proporcionar una huella digital del mismo documento. Para que sea una función checksum útil, no se debe poder encontrar una mensaje que concuerde con un valor especifico o encontrar dos mensajes que concuerden con el mismo valor. También son llamados Mensajes Digest. Debido a su unicidad, estos mensajes pueden ser sustituidos por el mismo mensaje bajo ciertas circunstancias. Por ejemplo, si otro servidor debe aplicar una etiqueta, el mensaje digest puede ser transmitido en lugar del mensaje original, reduciendo el trafico de red y mejorando la seguridad.

3.2.3 Confidencialidad y Firmas Digitales

Además de las llaves de distribución, los algoritmos de llave pública también ofrecen confidencialidad y Autenticación, el más conocido de estos algoritmos es el de firmas digitales.

Por ejemplo, Si **x** encripta su mensaje con la llave pública de **y**, entonces **x** puede estar seguro que sólo **y** puede desencriptar el mensaje con su correspondiente llave privada.

Una firma digital es un mensaje encriptado con la llave privada de quien envía, y es generada en dos pasos. Primero quien envía aplica una función hash unidireccional que produce un mensaje digest basado en el contenido del mensaje. Segundo, el que envía encripta el mensaje con su llave privada. El recipiente, para desencriptar el mensaje aplica la llave pública de quien envía y la misma función hash que puede autentificar al que envía y verificar si los datos fueron modificados mientras estaban en tránsito.

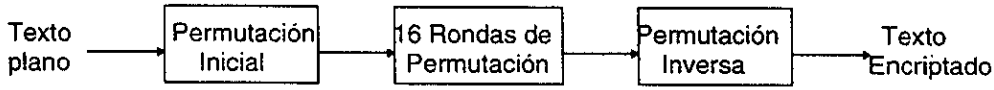
El tiempo es un factor sumamente trascendente en criptología, y ya que es imposible demostrar que un algoritmo es a prueba de ataques ya que estos se basan casi siempre en la fuerza bruta (por lo que no es posible descubrir posibles debilidades durante la etapa de prueba o validación), lo que nos garantiza que si eventualmente alguien rompe nuestro cifrado - habrá pasado tanto tiempo que quizá ya no existamos para poder enterarnos.

En la siguiente parte trataré de explicar a grandes rasgos algunos fundamentos teóricos en los que se basan algunos algoritmos de encriptación.

"..... En el fondo toda la encriptación se puede reducir conceptualmente a una función matemática que establece una relación uno a uno entre el conjunto de todos los posibles mensajes legibles y otro conjunto, de igual número de elementos, en el que los mensajes no son inteligibles....." [MALLÉN 1996].

3.3 Algoritmo DES

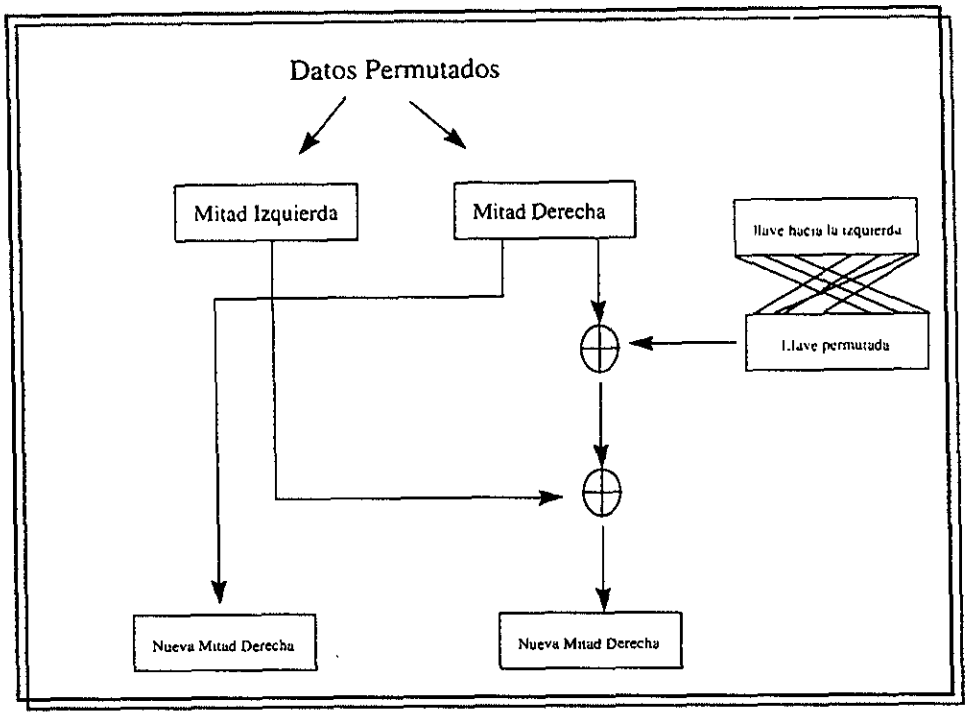
Para mediados de 1970 IBM desarrollo un algoritmo de encriptación DES (data encription standard). DES no es un algoritmo trivial, sino más bien bastante complejo, y muchos de sus consideraciones de diseño no son evidentes. El propósito de DES es proveer una forma eficiente de encriptar y desencriptar texto de tal forma que sea impenetrable para extraños. La funcionalidad básica de DES es el de una permutación inicial del texto plano, seguido por 16 rondas de substituciones y permutaciones, terminando con una permutación inversa final, que da como resultado el texto encriptado.



El algoritmo DES trabaja en bloques de 64 bits de entrada y hace uso de una llave de 56 bit como parte del proceso de encriptación. Conforme se llega a la 16 ronda de substitución y transposición, una llave de 48 bit se deriva de la llave de 56 bits.

A continuación esta los pasos que se deben seguir en el algoritmo DES :

1. El texto se divide en bloques de 64 bits.
2. El bloque de 64 bits es permutado.
3. Los bloques de datos de transforman usando una llave de 64 bits (de los cuales sólo se utilizan 56, se eliminan los bits múltiplos de 8; es decir 8, 16,24, 32, 40, 48, 56, 64).
4. Se inicia una secuencia de operaciones llamada ciclo
    - Los 64 bits permutados se dividen en 2 mitades de 32 bits.
    - La llave se recorre 1 o 2 bits dependiendo de la vuelta en la que se encuentre el ciclo. Las vueltas 1, 2, 9 y 16 se recorren un bit, las demás se recorren 2 bits.
    - La llave se combina con la mitad derecha y el resaltado se combina con la mitad izquierda. El resultado de estas combinaciones será la nueva mitad derecha, así mismo la vieja mitad derecha es la nueva mitad izquierda. La siguiente figura ilustra el proceso.



Un ciclo en DES

5. Cada ciclo es repetido 16 veces..
6. Después del ultimo ciclo, existe una permutación final que es la inversa de permutación inicial.

Operaciones en el texto

Expansión y permutación

1. Cada mitad derecha se expande de 32 a 48 bits mediante la expansión permutación los bits 1 y 4 se duplican.

bit	1	2	3	4	5	6	7	8
movimiento	2,48	3	4	5,7	6,8	9	10	11,13
bit	9	20	11	12	13	14	15	16
movimiento	12,14	15	16	17,19	18,20	21	22	23,24
bit	17	18	19	20	21	22	23	24
movimiento	24,26	27	28	29,31	30,32	33	34	35,37
bit	25	26	27	28	29	30	31	32
movimiento	36,38	39	40	41,43	42,44	45	46	47,1

2. Transformación de la llave, de la llave de 64 bits se eliminan los múltiplos de 8, la llave se divide en dos mitades de 28 bits, las mitades se recorren de manera circular un número determinado de posiciones

3. Se pegan las dos mitades y se seleccionan 48 bits de los 56 y se permutan, con lo que se tiene la llave utilizada en el ciclo en el que se esta.

bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14
posición seleccionada	5	24	7	16	6	10	20	18	-	12	3	15	23	1
bit	15	16	17	18	19	20	21	22	23	24	25	26	27	28
posición seleccionada	9	19	2	-	14	22	11	-	13	4	-	17	21	8
bit	29	30	31	32	33	34	35	36	37	38	39	40	41	42
posición seleccionada	47	31	27	48	35	41	-	46	28	-	39	32	25	44
bit	43	44	45	46	47	48	49	50	51	52	53	54	55	56
posición seleccionada	-	37	34	43	29	36	38	45	33	26	42	-	30	40

4. Esta llave se combina mediante la función XOR con la mitad derecha expandida (32 a 48). El resultado se mueve a las cajas S.

Cajas S

Las cajas S realizan una substitución basada en una tabla de 4 renglones y 16 columnas. Supóngase que el bloque B_j tiene los bits b_1,b_2,b_3, b_4, b_5 y b_6. Los bits b_1 y b_6 se toman para formar un numero binario de 2 bits, b1b6 (de 0 a 3) y llamaremos r; los bits b_1,b_2,b_4 y b_5 forman un número binario de 4 bits (0-15) que llamaremos e. La sustitución de las cajas S transforman cada bloque B_j de 6 bits en 4 bits mediante la intersección del renglón r y la columna c de la sección S_i de la tabla de las cajas S del DES.

		Columnas															
Caja	Linea	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	13	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7																
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																	
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	8
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

B7=010011 r=01=1, c=1001=9, la intersección de r y c es 3 por lo tanto 010011 se sustituye por 001.

Permutación inicial y final

La permutación inicial reordena los 64 bits de cada bloque de entrada de acuerdo a la siguiente tabla :

Bit								
posición	40	8	48	16	56	24	64	32
	1	2	3	4	5	6	7	8
Bit	39	7	47	15	55	23	63	31
posición	9	10	11	12	13	14	15	16
Bit	38	6	46	14	54	22	62	30
posición	17	18	19	20	21	22	23	24
Bit	37	5	44	13	53	21	61	29
posición	25	26	27	28	29	30	31	32
Bit	36	4	44	12	52	20	60	28
posición	33	34	35	36	37	38	39	40
Bit	35	3	43	11	51	19	59	27
posición	33	34	35	36	37	38	39	40
Bit	34	2	42	10	50	18	58	26
posición	49	50	51	52	53	54	55	56
Bit	33	1	41	9	49	17	57	25
posición	57	58	59	60	61	62	63	64

Al final de la ultima ronda de sustitución/permutación se realiza una permutación final (inversa a la permutación inicial) mediante la siguiente tabla :

Bit posición	58 1	50 2	42 3	34 4	26 5	18 6	10 7	2 8
Bit posición	60 9	52 10	44 11	36 12	28 13	20 14	12 15	4 16
Bit posición	62 17	54 18	46 19	38 20	30 21	22 22	14 23	6 24
Bit posición	64 25	56 26	48 27	40 28	32 29	24 30	16 31	8 32
Bit posición	57 33	49 34	41 35	33 36	25 37	17 38	9 39	1 40
Bit posición	59 41	51 42	43 43	35 44	27 45	19 46	11 47	3 48
Bit posición	61 49	53 50	45 51	37 52	29 53	21 54	13 55	5 56
Bit posición	63 57	55 58	47 59	39 60	31 61	23 62	15 63	7 64

3.4 Merkle Hellman

El algoritmo de Merkle-Hellman knapsack, es un algoritmo representativo de los algoritmos basados en problemas muy difíciles.

Cuando hablamos de problemas difíciles (complejidad) no nos referimos a lo complicado o fácil que puede ser el problema (ya que esto es subjetivo, lo que es fácil para una persona puede ser difícil para otra), sino más bien hablamos de tiempo y recursos necesarios (en cómputo) para realizar una tarea. En especial la complejidad se refiere al tiempo que tarda una máquina en realizar una tarea. La complejidad a la que nos referiremos a través de este trabajo será la complejidad que se da en el peor de los casos o big 0.

La complejidad O, puede ser constante O(1); lineal O(n), cuadrada O(n2); logarítmica O(logn); exponencial O(2n).

Existen problemas que una computadora puede resolver en millonésimas de

segundo, pero existen otros que por su naturaleza la misma máquina se tardaría varios miles de años en resolverlos.

La idea fundamental del algoritmo M-H knapsack, es el tener un algoritmo que encripte la información, de tal forma que si alguien intenta decodificarla sin las herramientas necesarias (llaves) le tome varios años el llegar a la solución correcta, y para entonces lo más probable es que la información sea obsoleta.

La forma en como funciona a grandes rasgos este algoritmo es tener dos llaves, una privada que se utilizara para desencriptar y una pública con la cual se encriptará la información.

Este sistema, de llave pública también es llamado sistema de encriptación asimétrico. Cada usuario tiene dos llaves: una llave pública y una llave privada. Un usuario puede decodificar con una llave privada lo que alguien encripto con la llave pública.

El algoritmo esta basado en el problema knapsack, que es un principio matemático, y consiste en tener un conjunto de enteros positivos y un número llamado suma objetivo, y la meta es encontrar el subconjunto de enteros que sumados lleguen a la suma objetivo, encontrando así las llaves pública y privada. Este problema tiene la característica de ser NP-completo, o sea que para ser resuelto requiere de un tiempo exponencial al tamaño del problema.

La idea base del Merkle-Hellman es codificar un mensaje binario, reduciendo el texto cifrado a la suma objetivo obtenida a través del resultado de añadir los términos que corresponda con 1 en el texto plano, es decir, se convierten bloques de texto plano en una suma knapsack añadiendo a la suma los términos que concuerden con los bits 1 en un texto plano.

Un knapsack se representa como un vector de términos enteros en los cuales el orden de estos es muy importante. Existen dos knapsacks: el knapsack fácil(se resuelve en tiempo linear) para el cual existe un algoritmo rápido y el knapsack difícil, derivado de modificar los elementos del knapsack fácil.

Para obtener el knapsack simple:
Se elige un entero inicial a, se elige un numero siguiente más grande que el anterior (b donde b>a), luego se selecciona un entero más grande que la suma del primer y segundo entero (c donde c > (a+b)). Todo se realiza en forma aleatoria

Ejemplo:

Secuencia	Suma	Termino Siguiente
1		
1	1	2
1,2	1+2=3	4
1,2,4	1+2+4=7	9
1,2,3,9	1+2+4+9=16	19

Tomando la secuencia resultante tenemos que el knapsack ={1,2,4,9,19}

Una vez elegido el simple knapsack se elige el hardknapsack de la siguiente manera:

1.-Se elige un múltiplo w y un módulo n, el múltiplo no debe tener factores comunes con el modulo (para esto se debe elegir un modulo primo) el modulo que se elija deber ser más grande que el entero más grande del simple knapsack.

2. Se reemplaza cada término del simple knapsack con la fórmula

$$h_i = w * s_i \bmod n$$

entonces para S=[1,2,4,9* con w=15 y mod 17 tenemos que :

H = {(1*15)mod 17,(2*15)mod17,
(4*15)mod 17,(9*15)mod17}

Una vez que se tiene la llave pública H y la llave privada S podemos empezar a encriptar.

Si tenemos un texto plano llamado P, lo vamos a dividir en bloques de m bits cada uno, en donde m representa el número de enteros que tiene el knapsack

Si P=[0100][1011][1010][0101]

0100 * 1513916=13
1011 * 1513916=40
1010 * 1513916=24
0101 * 1513916=29

Lo que nos da el mensaje encriptado de P=[13,40,24,29]

Para desencriptar tenemos que:

S=1, 2, 4, 9
w=15
n=17
P=13, 40, 24 y 29

Para obtener el inverso de 15 mod 17 se hace:

$$15^{-1} \bmod 17 = 15^{17-2} \bmod 17$$
$$= 15^{15} \bmod 17$$
$$= 8$$

$$P_i * 8 = x_i \bmod 17 = x' = P_i'$$

$13 * 8 = 104 \bmod 17 = 2 = [0100]$
$40 * 8 = 320 \bmod 17 = 14 = [1011]$
$24 * 8 = 192 \bmod 17 = 5 = [1010]$
$29 * 8 = 232 \bmod 17 = 11 = [0101]$

Debilidades

Este método parece bastante seguro, con valores apropiados para n y m, es decir bastante grandes, así las oportunidades de romper el método mediante fuerza bruta, es decir probando cada posibilidad de solución, es imposible.

Sin embargo, un interceptor no tiene que resolver el problema básico del knapsack para romper la encriptación, porque esta depende de determinadas instancias del problema. Se encontró que si el valor de n llega a ser conocido, puede ser posible determinar el knapsack simple.

3.5 Algoritmo RSA

Otro algoritmo importante en el manejo de llaves es el RSA (debe su nombra a Rivest, Shamir y Adleman) está basado en el hecho de que la factorización de números compuestos con factores primos muy grandes requiere de una cantidad abrumadora de cálculos. De hecho la experiencia ha demostrado que éste es un problema no computable (NP).

El algoritmo RSA es similar al método Merkle-Hellman, en lo concerniente en que es necesario se deben encontrar cantidades que deben sumar un número determinado o deben multiplicarse por un producto determinado.

Utilizan dos llaves para encriptar y desencriptar d y e, las cuales pueden ser intercambiables. Un bloque de texto plano P es encriptado como $P^e \ mod \ n$. El problema de factorización es resuelto en tiempo exponencial.

La forma en como funciona es la siguiente:

- Un número p se llama primo si sus únicos divisores son +1, -1, +p, -p, de otra forma se llama compuesto.

- Todos los primos son nones, excepto el 2

  Todo número compuesto puede ser factorizado en factores primos, por ejemplo el 999999 puede ser factorizado por los números primos 3, 7, 11, 13, 37:

  999999=3*3*3*7*11*13*37

  Para describir el algoritmo RSA será necesario definir antes lo siguiente :

  - p y q son primos (secreto)
  - r = p*q (público)
  - f(r) = (p - 1) (q - 1) (secreto)
  - SK es la llave privada (secreto)
  - PK es la llave pública (público)
  - X es el mensaje (texto plano) (secreto)
  - Y es el texto cifrado (público)

  El algoritmo RSA requiere de aritmética modular.

Utiliza el principio de congruencia de Gauss:

Dos enteros a y b son congruentes para el módulo m si su diferencia a -b es divisible por el entero m, y se expresa :

$$a \equiv b \pmod{m}$$

- Cuando a y b no son congruentes se les llama incongruentes para el módulo m, y se expresan de la siguiente manera:

$$a \neq b \pmod{m}$$
$$b = a + cm \qquad (1)$$

- El algoritmo RSA está basado en una extensión del teorema de Euler, el cual establece:

$$a^{\phi(r)} \equiv 1 \pmod{r} \qquad (2)$$

donde:

1. a deber ser primo relativo a r. (los enteros a y b son primos relativos si su máximo común divisor, mcd, es 1.)
2. $\phi(r) = r(1-1/p_1)(1-1/p_2).....(1-1/p)$ donde p,p ..., p son factores primos de r. $\phi(r)$ es la función de Euler ϕ de r (también llamado indicador), que determina cuantos números 1, 2, ..., r son primos relativos de r.

- Para obtener una relación matemática entre las llaves pública y privada, PK y SK, el resultado de Euler se extiende como sigue. Primero, está demostrado que $a \equiv b \pmod{m}$ implica que $a^n \equiv b^n \pmod{r}$ para cualquier exponente m. Por lo tanto la fórmula de Euler $a^{\phi(r)} \equiv 1 \pmod{r}$, puede ser reescrita como:

$$a^{\Pi\phi(r)} \equiv 1 \pmod{r} \qquad (3)$$

donde a es primo relativo a r. Del hecho de que $a \equiv b \pmod{m}$ implica que $ac \equiv bc \pmod{m}$ para cualquier entero c y de la ecuación 3, se tiene que :

$$X^{\Pi\phi(r)+1} \equiv X \pmod{r} \qquad (4)$$

donde el texto plano X es un primo relativo a r.

- Sea PK y SK seleccionadas de tal manera que:

$$SK * PK \equiv m\phi(r) + 1 \qquad (5)$$

o, equivalente,

$$SK^*PK \equiv 1(m\phi(r)) \qquad (6)$$

- La ecuación 4 puede ser reescrita como

$$S\uparrow(SK * PK) \equiv X \ (m\ r)$$

la cual es cierta para cualquier texto plano (X) que es primo relativo del módulo (r).

- El cifrado (E) y descifrado (D) puede ser interpretado como :

$$Epk(X) = Y\ X\uparrow PK (mod\ r) \quad (7)$$

$$Dsk(Y) \equiv Y\uparrow SK (mod\ r) \equiv X\uparrow (PK*SK) (mod\ r) \equiv X (mod\ r) \quad (8)$$

y ya que la multiplicación es una operación conmutativa, se puede ver que el cifrado seguido de decifrado es equivalente al decifrado seguido del cifrado:

$$DSK(Epk(X)) = Epk(Dsk(X)) \equiv X (mod\ r) \quad (9)$$

Esta propiedad es útil para la generación de firmas digitales.

AL igual que el algoritmo de Merkle-Hellman, el método RSA ha sido analizado intensamente por personas dedicadas a la seguridad de cómputo, y realmente han sido pocos los problemas que se han identificado con el. Razón por la que es actualmente ampliamente utilizado para el uso de comunicaciones seguras.

3.6 Algoritmos Hash

Este algoritmo sirve para ver si algún archivo ha sido modificado sin autorización, la forma en como funciona es la siguiente, se corre el algoritmo hash y el resultado se guarda, después se vuelve a correr y el resultado se compara con el anterior. Si los dos resultados son diferentes, ocurrió un cambio en los datos y si el resultado es el mismo lo más probable (aunque no 100% seguro) es que no exista modificación alguna.

El resultado que produce la función Hash es un forma compactada de los datos originales, así que cualquier cambio a los datos resultara también en un cambio a la forma reducida del producto de la función hash. Este resultado también es llamado **DIGEST** o valor verificado.

Descripción de los Algoritmos HASH

Un ejemplo simple de las funciones hash es la función de o exclusivo de todos los bits de los datos. Este resultado reduce los datos a un sólo bit. Pero con sólo un bit como resultado, se esperaría que la mitad de todo el conjunto de datos produzca un valor hash entre 0 y la mitad de 1. Por lo que, cualquier cambio en los datos sólo tendrá una probabilidad de 0.5 para poder cambiar el valor hash.

En contraste, si los datos consisten en 8 bits, y la función hash es calcular el or exclusivo de todos los bytes, existen 2↑8 o 256 formas diferentes de valores hash. Por lo que cualquier cambio a los datos tendrá una probabilidad de 1/256≡0.003906 de no causar cambio en el resultado del valor hash. Como ya mencionamos, una función hash reduce una gran cantidad de datos en un resultado pequeño, llamado digest. En general, mientras más pequeño sea el digest, más valores se tienen que mapear a cada valor digest, y mayor es la probabilidad de cambios en los datos produzcan un cambio en el digest. Por esta razón, los digest tienden a ser pequeños (ente 100 y 1000 bits).

Estos algoritmos son fáciles de invertir, lo que quiere decir que un atacante puede determinar a simple vista cual seria el resultado de un cambio.

Una función hash criptográficas, utiliza un función de encriptación como parte de la función hash y el que envía puede calcular el valor hash de un bloque de datos para ser comunicado y enviado tanto los datos como el valor hash. Quien recibe la información tendrá acceso a la función encriptada y podrá calcular el valor hash de los datos recibidos. Un intruso podría modificar los datos o el valor hash incluso ambos, pero si desconoce la función criptográfica hash le seria difícil modificar ambas de tal manera que puedan llegar a coincidir.

Algoritmo Hash Seguro

Para proveer de un estándar para firmas digitales. Se creo el Secure Hash Algorithm. Este algoritmo toma como entrada datos de una longitud menos de 2↑64 bits que son reducidas a 160-bit digest.

Cuando se tiene la función S(v,n), significa que cada bit es movido n posiciones a la izquierda, en dirección al bit más significativo. Todas las adiciones se realizan en mod 2↑32.

Primero el mensaje se inicia con un 1, y se rellena con 0's, teniendo un valor de 64 bits.

3.7 Confianza en los Métodos Criptográficos

Los métodos de encriptación deben ser robustos para generar confianza en su uso en sistemas de comunicación e información. Su uso se debe regular a través de licencias, métodos y para hacerlos aun más confiables los gobiernos de todos los países deberían emitir leyes al respecto.

3.8 Elección de los Métodos de Encriptación

Los usuarios deben tener acceso a métodos de encriptación que satisfagan sus necesidades, de manera que estén en condiciones de enviar y recibir información de manera integra y confidencial, y son estos usuarios quienes deben determinar el tipo y nivel de seguridad que requieren y las formas de encriptación adecuados incluyendo un manejo de sistema de llaves, estos sistemas deben considerarse este asunto como sujetos de ley.

Los gobiernos deben ser los encargados del control emitiendo leyes y estándares de los métodos de encriptación, pero respetando la elección de los usuarios en cuanto al método que les conviene.

El desarrollo de los métodos de encriptación debe ir de acuerdo con el desarrollo de la tecnología, la demanda de los usuarios y los sistemas de seguridad existentes en cuanto al uso de comunicaciones.

Tanto los gobiernos, como los particulares así como los encargados del desarrollo de los protocolos deben cooperar para establecer los estándares de los métodos de encriptación y protocolos de comunicación, y en caso de que existan estándares o protocolos nacionales, hacer que compaginen con los protocolos o estándares de encriptación internacionales para permitir la portabilidad, movilidad e interoperabilidad entre ellos; también se deben desarrollar mecanismos que evalúen que se cumpla con dichos protocolos y estándares.

La guía para la protección de la privacidad y flujo de datos personales OECD, prevee una serie de reglas concernientes para el manejo de información personal y debe aplicarse en concordancia con las leyes nacionales para implementar los protocolos de comunicación junto con los estándares de encriptación.

3.9 Protocolos

Cuando una computadora entra en comunicación con otras necesita saber con quien se esta comunicando y también debe saber cuando "hablar" y cuando "escuchar". Para lograr esto requerirá de una serie de pasos que se ejecutaran en una forma ordenada, a esta serie de pasos se le llama protocolo. Todos las partes involucradas en una comunicación deben conocer perfectamente el protocolo a través del cual lograran llegar a un acuerdo.

Los protocolos pueden ser propietarios o estándares. Los protocolos propietarios, son las especificaciones de los protocolos desarrollados por empresas privadas, quienes tiene derechos legales para hacerle cualquier tipo de modificación. Los protocolos estándar, son desarrollados por comités internacionales de estándares, y cualquier modificación debe ser aprobada por estas comisiones.

Características de un protocolo:

- Deber ser establecido por adelantado.
- Mutuamente suscrito. Todos las partes están de acuerdo.
- Inambiguo. Nadie puede fallar en algún paso.
- Completo. Debe seguir todos los pasos hasta llegar a su fin.

Existen varios tipos de protocolos, y dependiendo del tipo de actividad que se realice será el protocolo que se utilizara, por ejemplo existen protocolos para negociar contratos, protocolos para llevar a cabo una votación, protocolos para distribuir información, etc. Muchas de estas tareas, debido a la importancia que llegan a representar, necesitan ser llevadas a cabo con testigos para asegurar que no existe ningún tipo de fraude por ninguna de las partes o incluso asegurarse que nadie más tome parte en estas transacciones.

La sociedad actualmente requiere del uso de computadoras y telecomunicaciones como herramienta diaria no sólo para realizar actividades laborales sino también como recreo y otras muchas actividades de tipo personal

como la venta y compra de productos. Para efecto de llevar acabo todas estas tareas efectivamente se deben desarrollar protocolos por los cuales las partes involucradas puedan interactuar entre ellas con la seguridad que nadie será defraudado.

Además de regular el comportamiento de la comunicación, los protocolos tienen otro propósito, separar el diseño de la aplicación proceso de completar una tarea del mecanismo por el cual esta es hecha. Un protocolo especifica sólo las reglas de comportamiento que nos sirven para saber que llegamos al resultado que esperábamos.

El diseño del protocolo tiene que ser diferente del diseño de la implementación, lo que es una importante ventaja, porque después se puede cambiar cualquiera de los dos sin afectar al otro. Existen tres niveles de protocolos: los protocolos arbitro, los adjudicados y los autoreforzados, a continuación se da una breve descripción de cada uno:

Protocolos Arbitro

Un arbitro, se refiere cuando existe una tercera parte que en forma desinteresada y en forma confiable ayuda a completar una transacción entre dos partes (por ejemplo, una autoridad certificadora). En casos como la venta de un carro en el que interactuan dos extraños, quienes desconfían uno del otro, se podría utilizar a un abogado o a un banco como arbitro, que certifique el dinero no será entregado al vendedor hasta que el carro este en manos del comprador. En un protocolo de computación, un arbitro es la tercer parte que asegura que la operación es justa (legal) para ambas partes. Este arbitro puede ser una persona, un programa o una máquina. Un ejemplo de esto es en una red en la que esta corriendo un programa en una de sus maquinas, dicho programa recibe u manda un mensaje entre los usuarios, así que, cuando un usuario recibe un mensaje de A, si este mensaje vino del programa arbitro, entonces realmente viene de A.

Esta noción de arbitro es la base para un tipo de protocolo llamado protocolo arbitro. Sin embargo, este protocolo tiene algunas fallas, por lo que se debe evitar su uso:

- Las dos partes involucradas quizá no encuentren una tercera parte neutral en la cual ambos puedan confiar.

- El tener un arbitro en la red, representa un costo a los usuarios en la red, el cual puede llegar a ser muy alto.

- Los árbitros causan demora en las comunicaciones, debido a que una tercer parte involucrada debe recibir la información y después enviarla.

- La confidencialidad se vuelve vulnerable, porque los árbitros tienen acceso a mucha información considerada sensible.

Protocolos Adjudicados

Este protocolo es similar a la idea de un adjudicador: una tercera parte involucrada dispone de información suficiente para determinar si una operación fue justa o no. Esta tercera parte o adjudicador, no sólo puede determinar si la operación es valida o no, sino tomando en cuenta las reglas del protocolo, puede decidir si existió trampa. Este tipo de protocolo sólo se utiliza cuando existe disputa, o sea, sólo después que la operación fue efectuada.

Protocolos Autoreforzados

Este tipo de protocolos son los ideales, ya que garantizan equidad. Si cualquiera de las partes trata de hacer trampa, este hecho se hace evidente a la otra parte. No es necesario utilizar terceras partes para asegurar que las operaciones sean validas.

La desventaja existente es que no existen protocolos autoreforzados para cada situación.

3.9 Certificados

Una autoridad de certificación es aquélla con la que las entidades (usuarios u organizaciones) pueden registrarse y después de ser investigadas, se les otorga un certificado para autentificar que ellos son quien dicen ser. Un certificado es un dato formateado, firmado con la llave privada de CA, que atestigua la validez de la llave pública que esta en el certificado y su asociación con el principio de identidad

(usuario, organización). Esta autoridad además de tener una lista de certificados también tiene una de revocación de certificados

Los certificados digitales le dan a la gente, organizaciones y negocios en Internet una forma simple de verificar la identidad de la contraparte. Para los consumidores, algunas de las ventajas que los certificados les otorgan son:

- Una forma sencilla de verificar la autenticidad de una organización antes de darle algún tipo de información confidencial.
- Y la confianza de que si algo sale mal en alguna operación con quien están realizando una operación, tienen los elementos necesarios para establecer una demanda legal.

Para los negocios, las ventajas incluyen:

- Una forma de verificar la identidad de los individuos sin utilizar identificador de usuario y password, que son fáciles de olvidar y suelen compartirse entre los usuarios.

- En lugar de manejar grandes lista de identificadores de usuarios y paswords, las empresas pueden darle a cada uno de sus empleados un certificado, así los procesos que dan el acceso a los servicios sólo tendrán que validar la firma en el certificado.

- Los servicios que basan su autenticación en certificados tienen menores probabilidades de ser víctimas de abusos porque es más difícil compartir certificados y llaves compartidas que identificadores de usuario y passwords.

Tipos de Certificados

Existen 4 tipos de certificados digitales en uso por Internet, que son:

Certification Authority Certificates (Autoridades Certificadoras de Certificados).	Estos certificados contienen la llave pública de la autoridad certificadora que los emitió y el nombre de la autoridad o el servicio que están certificando, y puede ser firmado por ellos o por otra autoridad certificadora (Autoridad de Certificación Pública Primaria (PCA)). Algunas autoridades certificadoras son: AT&T, BBN, Canadá Post Corporation, CommerceNet, GTE CyberTrust Root, KEYWITNESS Canadá, MCI Mall RSA, Thawte Premium Server, etc.
Server Certificates (Certificadores de Servidores)	Estos certificados contienen la llave pública de un servidor SSL, el nombre de la organización que tiene el servidor, el nombre del servidor en Internet, y la llave pública del servidor.
Personal Certificates (Estos certificados tienen el nombre individual y la llave pública individual)	También pueden tener algún otro tipo de información como: dirección electrónica, dirección postal o algún otro tipo de dato importante.
Software Publisher Certificates (Certificados para Públicadores de Software)	Estos certificados se utilizan para firma el software que será públicado.

CAPITULO IV

Seguridad en Internet

En este capítulo trataré el tema de Internet, pero bajo la perspectiva que he venido desarrollando durante este trabajo, la seguridad. Primero, hago una pequeña descripción de que es, como funciona, algunos de los problemas de seguridad a los que se enfrenta sus posibles soluciones y finalizo describiendo un protocolo para establecer comunicación entre dos máquinas de forma segura.

4.1 Internet

Internet es una red de redes a nivel mundial desarrollada en 1969 por el departamento de defensa de Estados Unidos. Casi treinta años después, Internet o como también se le llama World Wide Web, esta al alcance de todo el mundo. Internet se podría definir como la red física y el Web es la parte lógica que hace uso de varios protocolos para establecer comunicación entre ellos, siendo el más utilizado el protocolo HTTP.

Con el continuo avance de la tecnología, Internet ha revolucionado la forma de intercambio de información y de hacer negocios. Primero solo hubo repositorios con documentos estáticos que evolucionaron a aplicaciones y transacciones en línea, lo que inevitablemente trajo consigo riesgos que amenazan el intervenir o modificar la información en flujo. Para asegurarse que las entidades que están interactuando pueden hacerlo sin exponer su información, es necesario establecer marcos de seguridad robustos. Antes de definir los marcos, quisiera comentar de forma breve como funciona WWW.

EL WWW se encarga de proveer de datos a una porción importante de la población mundial, en forma de documentos ligados que pueden incluir texto, gráficas, animación, audio, video, imágenes digitalizadas en 3era dimensión y para lograr la comunicación entre las máquinas ejecuta los siguientes pasos :

- Conexión. Un trata de establecer contacto con un servidor.
- Petición. Le solicita una sesión.
- Respuesta. El servidor responde si otorga o no la sesión.
- Termino de sesión. Ambos dan por finalizada la sesión.

Para hacer lo anterior existen los navegadores de Web, que también tienen entre sus funciones el decodificar documentos escritos en HTML, que hasta ahora ha sido el lenguaje estándar para el WWW. Estos documentos HTML pueden tener incorporados elementos mulitimedia y ligas hacia a otros documentos, en el mismo servidor o en algún otro. Estas ligas se representan por medio de un texto subrayado (ligas hypertext) o imágenes, y el tiempo que tardará un documento en desplegarse dependerá del tamaño del documento, del trafico en la red o la capacidad del hardware y en base a esto el tiempo puede darse en segundos. minutos e incluso horas. Para localizar estos documentos hace uso de los URL

(localizador uniforme de recursos) que son los elementos que nos dan la ruta de acceso a los recursos. El URL se divide en 4 partes: protocolo, dominio, ruta y nombre del archivo. El protocolo nos da la conexión. El dominio nos da el servidor y a que puerto se necesita hacer la petición de información. La ruta se va a dar después de la dirección del servidor y se separa por medio de "/". Por último se coloca el nombre del servidor. Un ejemplo :

http://servicio:puerto/directorio/archivo

4.1.1 Seguridad en Internet

La seguridad de las comunicaciones y las computadoras se puede dividir en 5 servicios básicos:

Servicio	Descripción
Servicio de Autenticación (Authentication Service)	Asegurarse de que las entidades son quienes dicen ser. La autenticación puede ser para personas (autenticación de entidad) o de información (autenticación de los datos de origen)
Servicios de Confidencialidad (Confidentiality Services)	Asegura que solo personas autorizadas tengan acceso a la información.
Servicios de Control de Acceso (Access Control Services)	Protege en contra de acceso no autorizado
Servicios de Integridad (Integrity Services)	Protección de modificación de la información sin autorización.
Evitar Negación (No Repudiation)	Recopilación de evidencias de transacciones para ser utilizadas en caso de que alguna de las partes que intervinieron niegue su participación.

El concepto de estos servicios de seguridad electrónicos en la mayoría de los casos no son nuevos, sino que se han derivado de otros, la tabla siguiente muestra algunos ejemplos:

Servicio de Seguridad	Medios de seguridad no electrónicos	Medios electrónicos de seguridad
Autenticación	Credenciales con fotografía y firma	Certificados Digitales
Control de Acceso	Candados y llaves Sistemas de llave maestra Guardias en los accesos	Roles y privilegios

Confidencialidad	Cartas selladas Envolturas obscuras Tinta invisible	Esquemas de encriptación
Integridad	Tinta indeleble Hologramas	Firmas Digitales
Evitar negación	Firmas notarias Correos registrados o certificados	Firmas Digitales

4.1.2 Procedimiento para obtener un certificado

Lo siguiente muestra los pasos que deben seguirse para obtener un certificado digital :

1	El usuario contacta con una Autoridad Certificadora y le solicita un certificado digital. Durante este proceso el usuario genera un par de llaves pública y privada. La llave privada es almacenada en el disco del usuario mientras la llave pública se envía a la autoridad certificadora con la petición. La llave privada nunca debe darse a conocer.
2	Con los datos que le proporciono el usuario a la Autoridad Certificadora, ésta verifica que el usuario es quien dice ser. Dentro de un ambiente Intranet esto puede ser hecho validando la información con el departamento de Recursos Humanos, pero en un ambiente Internet esta validación tiene que ser hecha a través de agencias de crédito.
3	Una vez que la Autoridad Certificadora ha obtenido la información positiva necesaria sobre el solicitante entonces expide el Certificado al usuario. El usuario una vez enterado de su aceptación, se conecta al sitio de Web de la autoridad Certificadora y baja su certificado, para instalarlo posteriormente en su navegador.
4	El servidor de aplicaciones también puede pedir un certificado de firma digital por parte de la autoridad Certificadora.
5	La Autoridad Certificadora valida al servidor solicitante y le expide un certificado.
6	Se instala el certificado del servidor.

El proceso que deben de seguir el cliente y el servidor para la autenticación es el siguiente:

1	Un cliente envía una copia de su certificado al servidor, el servidor responde enviando su propio certificado al cliente.
2	Ambas entidades utilizan la llave pública de la Autoridad de certificación para verificar que ambos certificados son validos
3	También revisan el la lista de revocación de la Autoridad de Certificación para asegurarse que sus certificados no han sido revocados
4	Ambas entidades generan un valor binario random que se utiliza una sola vez y lo encriptan con la llave pública de la otra entidad antes que se la envíen entre ellos
5	Ambas entidades utilizan sus llaves privadas para desencriptar el valor binario que recibieron.
6	Ambas entidades combinan el valor binario que recibieron con el que generaron para crear una llave hash
7	Ambas entidades utilizan la llame con el algoritmo RSA para generar una combinación hash de dos valores binarios y enviar este valor hash entre ellos.
8	Si las entidades descubren que el valor hash que reciben es igual al que enviaron, entonces están seguros que la otra entidad es autentica. Lo que permite al servidor otorgarle los permisos para accesar sus recursos de acuerdo al rango que les hayan sido concedido.

4.1.3 Servicios de Seguridad

Esta es una breve descripción sobre los servicios de seguridad mencionados.

Autenticación Básica

Permite que el servidor solicite al usuario un identificador de usuario y un password en el momento en que intente accesar una página o una aplicación protegida. Esta información sirve para ver la clase de privilegios que tiene o si es que los tiene. El usuario y el password viajan a través de la red por lo que sería conveniente el utilizar algún sistema como el protocolo SSL (secure socket layer, que se tratará más adelante) que permita enviar la información encriptada de tal forma que solo las máquinas que tienen el derecho puedan descifrar esta información.

Autenticación Digest

El protocolo de Autentificaron Digest es igual que la Autenticación básica excepto que este encripta el password en el momento de ser introducido. No todos los navegadores soportan este tipo de seguridad. Cuando se tiene comunicación con navegadores que no soportan la autenticación Digest, la pagina a ser autenticada por el servidor lo tomará como si fuera Autenticación Básica y los passwords serán enviados sin encriptar.

Restricción de Direcciones IP

Estas restricciones permiten o niegan el acceso a sitios Web preestablecidos. Las direcciones IP están organizadas jerárquicamente, y este mecanismo permite un control de acceso, tanto de inclusión como de exclusión a todo una parte del árbol. Por ejemplo, permitiendo el acceso a determinada dirección IP que inician con X:Y, entonces ese sitio permitirá la entrada a cualquier dirección que tenga el prefijo X:Y. Este tipo de seguridad debe usarse en combinación con algún otro método de autenticación.

Restricciones de Nombres de Dominio

En lugar de restringir el acceso por medio de direcciones IP, los sitios pueden reforzar el control vía dominios. Para simular una restricción de acceso jerárquico IP bajo este mecanismo, los administradores pueden especificar una cadena de restricción del tipo de XYZ.COM que permite tanto incluir como excluir a todos los

dominios de este estilo. Este mecanismo también debe ser implementado en combinación con otro método de autenticación adicional.

Protección de Máquinas Clientes

Un riesgo importante es cuando la máquina con el navegador tiene que ejecutar algún tipo de código y a veces éste puede contener algún tipo de virus que destruye la información o puede tomar recursos del sistema (memoria, tiempo de CPU, etc.) hasta el punto donde la máquina es inutilizada. La privacidad de los datos de una máquina cliente es algo que debe tomar como responsabilidad el propietario de la máquina. Por ejemplo, un caso de vandalismo, se podría dar cuando en el navegador llama a una aplicación que necesita ser abierta con algún procesador de la máquina y es durante este proceso que se introducen virus en la máquina.

Protección de los servicios de Registro

El sistema operativo Unix es muy flexible, lo que lo hace vulnerable a ataques, ya que todas estas características de flexibilidad al final se traducen en puertas a los atacantes.

Cada vez que se haga acceso a un servidor se debe registrar :

- Dirección IP y/o nombre del servidor de donde se esta navegando
- Tiempo en que se baja la información
- Nombre del usuario
- Petición URL
- Estado de la petición
- Tamaño de los datos pedidos

Protección de Password

Los password son los encargados de proveer protección basada en un palabra que solo el usuario sabe. La forma más simple de protección en un ambiente de red es encriptar el password durante la transmisión.

Autenticación de Servidor con Llave pública

Cualquier empresa que hace negocios a través de Web, generalmente utiliza el sistema de encriptación de llave pública/privada (mencionados en el capítulo 3), para asegurar a sus clientes que es un sitio confiable.

El papel de la autenticación es asegurar que tanto el cliente como el servidor saben con quien van a realizar la transacción y el tipo de transacción que van a realizar. Para cada transacción en Web se tiene un requerimiento de autenticación, aunque no siempre es necesario realizar esta opresión.

Algunos ejemplos de ello son:

- Si un usuario simplemente quiere ver un documento publico, no es necesario llevar a cabo ningún tipo de autenticación.

- Si se va a llevar a cabo una compra a través de la red, el comprador necesita confiar en que el vendedor es realmente quien dice que es, y el vendedor deberá proteger la transacción del pago. Por su parte el vendedor también tiene que confiar que el comprador esta autorizado a utilizar la tarjeta de crédito, y que la compra por lo tanto será cubierta por la tarjeta del comprador.

- En el caso de una transferencia multimillonaria tenga que ser autorizada, tanto el cliente como el servidor necesitan tener un alto nivel de confianza y referencias uno del otro.

EL nivel principal de protección en un sistema generalmente siempre es vía password. Si estos son infringidos se tiene acceso con todos los privilegios del usuario a la información de éste, y es peor si accesa varios servidores con el mismo password. Razón por la que es muy importante en todos los casos el observar las reglas de los passwords mencionados en el capítulo 2.

Para evitar el uso de password se puede utilizar un certificado de firmas digitales de una tercer parte involucrada, conocida como "Autoridad Certificadora", de las que hable al principio del capítulo. La empresa que hace la petición es responsable de asegurarse de la integridad y mantener en secreto el certificado y la llave asociada. El uso de las llaves involucra verificaciones criptográficass construidas sobre el software que va a accesar la información, quienes tendrán que validar la información mediante un certificado autorizado.

Los usuarios de Internet interesados en proteger la información de sus tarjetas de crédito no deberán hacer negocios con quien no provee una llave pública de autenticación de servidor. Aun si aparentemente se esta haciendo negocios con un vendedor certificado en un sitio seguro (que puede ser verificado en el formato que se despliega con el navegador Netscape), es posible que alguien compre o robe un certificado y desvíe el trafico en la red de un usuario legitimo a su propio sitio utilizando un ruteador. Para asegurarse el usuario puede abrir la ventana de Información de documentos y examinar el certificado del servidor. Si el nombre del servidor y la empresa coinciden como se espera, entonces es lo más seguro es que el certificado sea válido.

Las técnicas de seguridad que he venido mencionando nos ayudarán a que los usuarios que van a realizar alguna operación lo hagan con roles que tienen asignados y nada más. Esto también nos reforzara la confianza en el caso en que queramos autorizar a usuarios anónimos para leer la información que esta en las páginas de un servidor Web, pero que no que tengan acceso a otros archivos que están en nuestra máquina. En cuanto a la intercepción no autorizada de la información, actualmente existen muchas formas de proteger de esto a nuestros datos, algunas de ellas (las más utilizadas) son:

- Seguridad física de la red.
- Esconder la información importante en un texto carente de reelevancia.
- Encriptación de la información.

De estas técnicas, la encriptación es la más practica, porque proteger físicamente la red de Internet es imposible y el esconder la información sólo funciona si la gente de quien se esconde la información no lo sabe.

Una de las innovaciones en Internet es el SSL, un sistema de encriptación de información que funciona de manera automática y transparente para el usuario final. Este sistema encripta la información conforme va siendo enviada a través de Internet y la desencripta antes de ser utilizada.

Este sistema, a pesar de su reciente introducción, es una parte importante de la seguridad en el ambiente Web. Por lo que resta del capítulo, describiré en forma breve su funcionamiento, que si bien es algo complicado y tiene debilidades sirve como base para desarrollar otro esquema para el desarrollo de conexiones seguras. Otro razón por la que elegí hablar de este protocolo es que utiliza muchos de los temas que he venido desarrollando durante esta investigación, por lo que me resulto de gran interés el incluirlo.

4.2 SSL

El Secure Socket Layer SSL (capa de conexión segura), es un protocolo de propósito general para enviar información encriptada a través de Internet, y fue desarrollado por la empresa Netscape (dueña del navegador netscape) para promover el uso de comunicaciones seguras.

SSL (abreviación que utilizaré para referirme a este protocolo) es una capa que existe entre el protocolo TCP/IP y la capa de aplicaciones. TCP/IP envía información libre de errores entre dos computadoras (incluso entre dos procesos en la misma computadora), y la función del SSL es añadir a ese flujo de información algunas características de:

- Autenticación y no repudio del servidor, utilizando firmas digitales
- Autenticación y no repudio del cliente, utilizando firmas digitales
- Confidencialidad de los datos a través del uso de encriptación.
- Integridad de los datos a través del uso de código de autenticación de mensajes (MAC).

El SSL funciona a base de separación de tareas porque utiliza distintos algoritmos para la encriptación, autenticación e integridad de datos (principios básicos para obtener una comunicación sin amenazas).

Los protocolos de encriptación no funcionan a menos que las partes que entren en comunicación estén de acuerdo en los algoritmos que van a utilizar. Esta es una de las razones por las que el SSL es un protocolo extensible y adaptable. Cuando un programa que utiliza SSL intenta conectar otro, los dos programas comparan notas electrónicamente, determinando cual es el protocolo de encriptación más robusto que tienen en común y este sea el que utilizan. Este fase del protocolo se le llama SSL Protocolo de Capa de Saludo.

SSL hace uso de la encriptación de llave pública, los procesos que utiliza para encriptar como para desencriptar son operaciones que consumen mucho tiempo, el SSL en orden de evitar guarda la información como "secreto maestro" entre las conexiones, y esto es lo que evita el repetir este proceso para cada conexión cliente y el servidor. Permitiendo así, el establecer conexiones de forma segura para entablar comunicación sin necesidad de ejecutar mas de una operación de llave pública.

Otra gran ventaja del SSL es la autenticación para el lado del cliente y del servidor por medio de certificados digitales, aunque esta es una parte opcional del protocolo, las implementaciones actuales lo hacen obligatorio. Otra característica importante es que aunque fue hecho para correr bajo el protocolo de

comunicación TCP/IP, puede ser implementado en cualquier protocolo orientado a las conexiones.

La información encriptada no puede ser comprimida (debido a que la encriptación quita las repeticiones o similitudes), por lo que antes de ser encriptada tiene que ser comprimida y el SSL tiene varios algoritmos para la compresión de la información.

Una debilidad del SSL es que dismuye la velocidad de transmisión de la información causa de la encriptación de la llave pública, a pesar que ha tratado de evitarlo con el "secreto maestro". Se han reportado decrementos en la funcionalidad de la transmisión de información hasta del 50%, por lo que se recomienda que si se tiene información que no requiere de algún tipo de seguridad se mande de forma natural y solo se utilicen estas conexiones cuando se trata de información importante para las entidades.

El protocolo SSL tiene tres propiedades básicas para una conexión segura:

- La conexión es privada. Después del Saludo Inicial (handshake) se define el tipo de llaves secretas a ser utilizadas. Para la encriptación de los datos se utiliza la encriptación simétrica (DES).
- La identidad de la contraparte puede ser autentificada a través de criptografía asimétrica o de llaves públicas como el RSA.
- La comunicación es confiable. La capa encarga del transporte incluye una verificación de integridad.

Los beneficios del SSL son:

- Seguridad Criptográficas. El protocolo SSL debe establece comunicación segura entre dos entidades.

- Interoperabilidad. Los programadores independientes deben estar en condiciones de desarrollar aplicaciones utilizando el SSL que permita intercambiar exitosamente parámetros sin el conocimiento de sus códigos.

- Extensibilidad. Busca proveer de marcos en los cuales nuevas llaves públicas y métodos de encriptación que vayan surgiendo. Previniendo la necesidad de creación de un nuevo protocolo y evitar la necesidad de implementar una nueva biblioteca de seguridad.

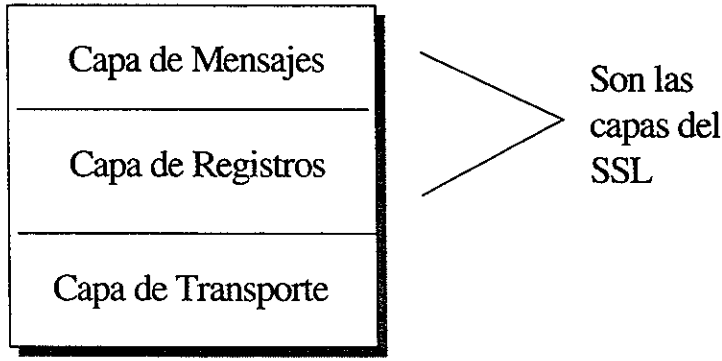
- Eficiencia. Las operaciones criptográficass tienden a utilizar de una forma intensiva, particularmente cuando se utilizan operaciones de llave pública, por lo que se ha incorporado un esquema de sesión que reduce el numero de conexiones, reduciendo también el trafico en la red.

El protocolo esta compuesto por dos capas. En el nivel mas bajo esta la capa que actúa con los protocolos de transporte (como TCP/IP) que es la SSL "Protocolo de Registro" (Record Protocol), esta capa se utiliza para la encapsulación de otros protocolos de mayor nivel. Uno de esos protocolos encapsulados es el SSL "Protocolo de Saludo Inicial" (Handshake Protocol) que permite la autentificacion entre el cliente y servidor, además de negociar el algoritmo y las llaves de encriptación antes de que el protocolo de aplicaciones transmita o reciba el primer byte de datos. Otra ventaja del SSL es que es independiente del protocolo de aplicaciones, además de ser transparente.

Todo esto se estructura de la manera siguiente:

- La capa de mensajes, que incluye a los datos de los usuarios, los mensajes de saludos, los mensajes de alerta y los mensajes de cambio de especificación de datos.
- La capa de registro, que fragmenta la información.

Ambas capas están sobre la capa de comunicación (que generalmente es el TCP/IP). Lo anterior se ilustra en la figura siguiente:



Atributos Criptográficos

Se utilizan cuatro tipos de operaciones criptográficass : firmas digitales, encriptación de cadenas, encriptación de bloques y encriptación de llaves públicas, los cuales se designa como digitally-signed, stream-ciphered, block-ciphered, block-ciphered y public-key-encrypted, respectivamente. El proceso de encriptación de un campo se especifica colgándole una etiqueta antes del tipo de especificación del dato.

Para la encriptación de digitally-signed, se utilizan las funciones hash unidireccionales como entrada para el algoritmo de firma, pueden ser RSA o DDS.

En la encriptación del tipo stream-cipher tiene como entrada un texto plano y como salida una cantidad de texto igual al de la entrada pero generada a través de un generador de números pseudorandom.

En la encriptación de block-ciphered, cada bloque de texto plano encripta a un bloque de texto cifrado. En la encriptación de llave pública, se utilizan funciones unidireccionales con "puertas falsas" para encriptar la información.

Sesiones y Estados de Conexión

El SSL se maneja a base de estados. Esta bajo la responsabilidad del protocolo Saludo Inicial coordinar los estados del cliente y el servidor, permitiendo que cada protocolo que trabaja en una máquina actúe en forma consistente, aun en el caso en que no se esta trabajando exactamente en una forma paralela. Lógicamente los estados se representan de una forma duplicada, la primera como el estado actual de operación y (durante el Protocolo de Saludo Inicial) se vuelve a presentar como un estado pendiente. También se mantienen estados de lecturas y escrituras de forma separada. Cuando el cliente o el servidor reciben un mensaje de cambio de especificación (change cipher spec), se copia el estado de lectura pendiente a un estado actual de lectura. Cuando el cliente o el servidor envían el mensaje de Cambio de Especificación, se copian los estados pendientes de escritura a estados actuales de escritura. Cuando el protocolo handshake termina la negociación, el cliente y el servidor intercambian mensajes change cipher spec e inician una comunicación con un nuevo cipher spec definido entre ambos.

Una sesión SSL puede incluir múltiples conexiones seguras, además de que las entidades pueden tener sesiones simultáneas.

Un estado de sesión incluye los siguiente elementos:

- Identificador de sesión. Se elige una secuencia de bytes arbitrarios para identificar el estado de una sesión.
- Certificado Pareja. Este elemento puede ser nulo
- Método de compresión. Que es el algoritmo que encripta la información antes de encriptarla.

- Spec Cipher (especificación de cifrado). Especifica el algoritmo de encriptación (puede ser null, DES, etc.). y un algoritmo MAC (puede ser MD5 o SHA). También define algunos atributos de la encriptación.
- Master Secret. Secreto de 48 bytes entre el servidor y el cliente
- Is resumable. Bandera que indique si la sesión puede o no iniciar nuevas conexiones.

Un estado de conexión incluye los siguientes elementos:

- Cliente y servidor random. Secuencia de bytes que eligen tanto el cliente como el servidor de forma aleatoria para hacer la conexión.
- Secreto de escritura MAC del servidor. Este método se utiliza en la información que escribe el servidor.
- Secreto de escritura MAC del cliente. Este método se utiliza en la información que escribe el cliente.
- Llave de escritura del servidor. La llave de encriptación de la información por lado del servidor y de desencriptación por lado del cliente.
- Llave de escritura del cliente. La llave de encriptación de la información por lado del cliente y de desencriptación por lado del servidor.
- Inicialización de vectores. Se inicializa un vector por cada llave. Este campo se inicializa primero por el protocolo SSL de handshake.
- Secuencia de números. Cada entidad mantiene una secuencia de números separada para transmitir y recibir mensajes en cada conexión. Cuando una entidad envía o recibe un mensaje de change cipher spec.

4.2.1 Capa de Registro

La primer capa del protocolo es la Capa de Registro. Esta capa envía bloques de datos, llamados registros, entre el cliente y el servidor. Cada bloque contiene hasta hasta 16,383 bytes de información. La representación de los datos se especifica como sigue:

Cada Registro SSL contiene la siguiente información:

- Tipo del contenido
- Versión del protocolo
- Longitud
- Información
- Códigos de Mensajes de Autenticación (MAC)

Cada registro es comprimido y encriptado de acuerdo a los algoritmo de compresión y encriptación actuales. Al inicio de una conexión, la función de compresión se define como nula al igual que la de encriptación. Ambos algoritmos

son inicializados durante la fase de saludos y pueden ser cambiados durante el curso de la conversación.

La función de códigos de Mensajes de Autenticación (MAC) es calculada mediante la formula de :

hash(MAC_write_secrete + pad_2 +
hash(MAC_write_secret + pad_1 + seq_num + lenght + content))

donde:

- MAC_write_secrete, es un secreto compartido entre el cliente y el servidor utilizado para validar la transmisión.

- pad_1, es un carácter hexadecimal arbitrario, que se utiliza como constante, para hacer los cálculos de la función MAC más seguros.
- pad_2, es otro carácter hexadecimal, que se utiliza de igual forma.
- seq_num, es la secuencia de numero del mensaje.
- hash, es el algoritmo hash actual, especificado en el mensaje de cifrado.

La capa de seguridad provee integridad para los datos. El uso de funciones MAC previene ataques dentro de una sesión SSL, porque cada mensaje tiene una secuencia única y la información va comprimida.

Protocolos SSL

Los protocolos SSL son tipos específicos de mensajes que son enviados utilizando la capa de registro, los protocolos son:

- protocolo de alerta
- protocolo de cambio de encriptación
- protocolo de saludo

Protocolo de Alerta

Las alertas son un tipo de mensajes específicos que pueden ser transmitidos por la Capa de Registro SSL. Las alertas están compuestas de dos partes: un nivel de alerta y una descripción de la alerta. Ambas codificadas como números de 8-bits.

Las alertas son encriptadas y comprimidas. Dentro del protocolos se definen dos niveles de alerta:

Nivel Alerta	Nombre del Nivel	Significado
1	Advertencia	Indican que ha ocurrido un problema que no es grave.
2	Grave	Las alertas graves terminan de forma inmediata con la sesión actual de SSL

Existen 13 definiciones de alertas:

Numero de Alerta	Nombre de Alerta	Significado
0	notificación de cierre	Indica el fin de sesión
10	mensaje inesperado	Se recibió un mensaje fuera de secuencia.
20	registro mac indebido	Se envió un registro con código incorrecto
30	falla de descompresión	La información de registro recibida fue incorrecta.
40	falla de saludo	Incapacidad de negociar un conjunto de parámetros de seguridad.
41	sin certificado	Si no existe certificado se envía éste mensaje.
42	certificado no válido	Si el certificado enviado de alguna manera se encuentra corrompido
43	certificado no soportado	Si el tipo de certificado no es soportado por el recipiente.
44	certificado revocado	Si se recibió un certificado que ya fue revocado.
45	certificado expirado	Si el certificado ya expiró
46	certificado desconocido	Cuando surge otro error durante el proceso de certificación
47	parámetros ilegales	Si se encuentra que algún valor en el protocolo de saludo está fuera de rango o es inconsistente.

Protocolo de Cambio de Encriptación

Se utiliza para cambiar de sistema de un método de encriptación a otro. Para hacer esto, el cliente y el servidor deben negociar un nuevo algoritmo de encriptación y nuevas llaves. Aunque este cambio ocurre al final del Protocolo de Saludo, también puede ocurrir en cualquier momento.

4.2.2 Protocolo de Saludo

El Protocolo de Saludo, se utiliza para autentificar al servidor con el cliente y viceversa, y para negociar los algoritmos iniciales de encriptación y las llaves que serán utilizadas.

Cuando un cliente se conecta a un servidor, el protocolo de Saludo Inicial. El SSL establece el protocolo que será utilizado durante la comunicación, selecciona los algoritmos de encriptación, autentifica a las entidades, y utiliza la llave de encriptación para crear un "secreto maestro", del cual las llaves de encriptación y autenticación son derivadas.

El secreto maestro para la sesión es creado por el servidor utilizando un pre-secreto maestro enviado por el cliente.

El secreto maestro se utiliza para generar cuatro llaves secretas:

- Una llave de encriptación utilizada para enviar información del cliente al servidor.
- Una llave de encriptación utilizada para enviar datos del servidor al cliente.
- Una llave de autenticación para enviar datos del cliente al servidor.
- Una llave de autenticación utilizada para enviar datos del servidor al cliente.

Secuencia de Eventos

El protocolo de saludo se ejecuta en 10 pasos (algunos opcionales {}):

1. El cliente abre una conexión y envía el saludo Hola-Cliente
2. El servidor envía el saludo Hola-Servidor
3. {El servidor envía su certificado}
4. {El servidor envía su intercambio de llave}
5. {El servidor envía una petición de certificado}
6. {El cliente envía su certificado}
7. El cliente envía un intercambio de llaves
8. {El cliente envía una verificación de certificado}
9. El cliente y el servidor envían mensajes de cambio de especificaciones.
10. El cliente y el servidor envían mensajes de terminación

Con la excepción de los secretos que son enviados encriptados, todo el protocolo de saludo es enviado sin encriptar. Los secretos se utilizan para encriptar todas las comunicaciones subsecuentes.

1) Hola-Cliente

El Hola-Cliente es un mensaje que contiene la información de la tabla siguiente:

Campo	Significado
Protocol Versión client_version	La versión más reciente del protocolo que soporta el cliente.
Random random	Estructura random que consiste en una etiqueta de 32 bits, de los cuales 28 son generados por un generador de secuencias random.
Session ID session_id	Este identificador de sesión, normalmente esta vacío para pedir una nueva sesión , si no esta vacío quiere decir que el cliente esta tratando de continuar una sesión previamente establecida.
CipherSuite cipher_suites<1...2^{16-1}>	Lista de los métodos de encriptación que soporta el cliente.
CompressionMethod compression_methods<1...2^{8-1}>	Lista de los métodos de compresión que el cliente soporta.

Después que el Hola-Cliente envía el mensaje, espera por el mensajes de Hola-Servidor.

2) Hola -Servidor

Cuando el servidor recibe el mensaje Hola-Cliente, responde con una falla de protocolo de saludo o con un mensaje Hola-Servidor.

En la siguiente tabla se muestran los mensajes Hola-Servidor:

Campo	Significado
ProtocolVersion client-version	Tiene la versión del protocolo utilizada por el cliente-
Random random	Estructura random que consiste en una etiqueta de 32 bits, de los cuales 28 son generados por un generador de secuencias random.
Session ID session_id	Este identificador de sesión, nunca esta vacío, si concuerda con algún valor anterior es que existe una sesión que quiere ser rehabilitada.
CipherSuite cipher_suite	El encriptado elegido por el servidor

	para esta sesión.
Compression_Method compression_method	Lista de los métodos de compresión elegidos por el servidor para esta sesión.

El servidor es quien elige el método de cifrado y el método de compresión a ser utilizado por la conexión. Si el servidor no implementa o no usa cualquiera de estos métodos de ofrecidos por el cliente, el servidor puede enviar una alerta de fallo de negociación y dar por terminada la sesión.

3) Certificados del Servidor

Después del enviar el servidor-hola, el servidor opcionalmente puede enviar su certificado.

4) Intercambio de llaves con el Servidor

El servidor envía el mensaje de intercambio de llaves, si el servidos no tiene certificado pueden suceder tres cosas:

- El servidor utiliza el protocolo de intercambio Diffie-Hellman
- El servidor utiliza el RSA
- El servido utiliza el Fortezza/DMS

5) Petición de Certificado

Si el servidor desea autentificar al cliente, puede enviar una petición al cliente.

6) El cliente envía un certificado

Cuando el servidor pide al cliente un certificado, este lo envía, y si no tiene envía una alerta de que no tiene certificado. Depende del servidor decidir que hacer si no hay alerta.

7) Intercambio de llaves del cliente

El cliente tiene tres tipos de llave para intercambio de mensajes pero solo puede enviar una que eligirá dependiendo del tipo de algoritmo de llave pública que haya sido seleccionado por el servidor.

8) Verificación de certificados

Este mensaje es utilizado para dar una verificación explicita del certificado del cliente, este mensaje solo es enviado si el certificado del cliente tiene capacidades de firma, consiste en dos mensajes de autenticación de códigos.

9) Especificación de cambio de cifrado

Después que es enviado el certificado de verificación es enviado. Todos los mensajes subsecuentes son comprimidos y encriptados de acuerdo al cifrado y los métodos de compresión especificados.

10) Terminación

El Mensaje de Terminación verifica que tanto el cliente como el servidor están en *sincronización. Si no lo están la liga es terminada.*

Capa de aplicación

Después que el mensaje de terminación ha sido enviado, los datos de aplicación son transportados. Estos datos son comprimidos y encriptados bajo los métodos actuales de compresión y encriptación.

Consideraciones

Cálculos Criptograficos

El intercambio de llaves, la encriptación, la autenticación y los algoritmos MAC son determinados por el mensaje de especificación de cifrado que haya sido seleccionado por el servidor y revelado por el mensaje Hola-Servidor.

Cálculos Criptograficos Asimétricos

Los algoritmos simétricos utilizados en el protocolo de saludo para autentificar las entidades y generar las llaves y los secretos compartidos. El algoritmo que se utiliza para convertir el secreto pre-maestro en un secreto-maestro, es el mismo. El secreto pre-maestro debe ser borrado de la memoria una vez que el master_secret haya sido calculado.

RSA

Este algoritmo se utiliza para generar el secreto pre-maestro por el cliente, que es encriptado por la llave pública del servidor. El servidor desencripta con su llave privada el secreto pre-maestro. Ambas partes convierten el secreto pre-maestro en *el secreto maestro*

Cálculos Criptograficos Simétricos

Esta técnica se utiliza para encriptar y verificar la integridad de los registros del SSL especificados por el estado activo actual del mensaje de especificación de encriptación.

El secreto Maestro

Antes que la verificación de encriptación o de integridad sean llevados a cabo en los *registros, el cliente y el servidor necesitan generar un secreto compartido.* Con una longitud de 48 bytes. Este se utiliza para generar llaves y secretos para la encriptación de los cálculos MAC.

Conversión del Master Secret en llaves y secretos MAC

El secreto maestro pasa a través de una función hash para convertirse en una secuencia de bytes seguros, que son asignados a los secretos MAC y llaves.

MAC

Se utiliza algoritmos hash para crear estos Códigos de Autenticación de Mensajes, que nos sirven para encriptar la información.

Este protocolo utiliza algoritmos complejos (lo que lo hace un tanto complejo de entender) para evitar que la información sea descifrada, pero esta misma seguridad hace que el flujo de la información sea lenta; lo que nos tiene que hacer pensar que tenemos que seguir buscando nuevas alternativas para que nuestras comunicaciones sean seguras y lo más eficiente posibles.

Conclusiones

La seguridad de nuestros sistemas de cómputo, y por consiguiente de nuestra información, antes de tener sustento en las técnicas de seguridad, se basa en el conocimiento del problema, y el que cada uno de nosotros nos hagamos responsables de ésta tarea; y si en el lugar donde realizamos nuestras actividades ya existen medidas precautorias, cooperar para que sean efectivas y si no las hay tomar las propias (en lo concerniente a nuestras labores y sin afectar a los demás) o sugerirlas a las personas encargadas.

Las técnicas de seguridad son muchas y muy variadas, el uso de ellas dependerá totalmente de las circunstancias, de lo que queramos proteger y de quien lo queremos proteger.

Tanto la encriptación y los protocolos son una muy buena opción para mantener nuestras comunicaciones seguras, ya que si alguien la intercepta sólo verá basura que de poco o nada le sirve. Y si podemos utilizar firmas digitales en lugar de passwords para accesar los sistemas, vamos a disminuir muchos riesgos de acceso no autorizado.

A pesar de que han sido y son muchos los esfuerzos por mantener la información intacta también existe mucho empeño por parte de los agresores por que no sea así, pero en la medida que seamos más precavidos menores serán los riesgos que correremos.

Bibliografía

Abrahams, M., y Podell, H.
Computer and Network Society
IEEE Computer Society Press
1987.

Bell, D.
Secure Computer Systems: A Retrospective
IEEE Computer Society Press
1983.

Cheswick, B., y Bellovin, S.
Firewalls and Internet Security
Adison Wesley
1994.

Davir, R.
A New View of Intellectual Property and Software.
Comm ACM, v39 n3.
Mar 1996, pp 21-30.

Eco, H.
Como se hace una tesis
Gedisa
1996.

Popek, G. y Klyne, C.
Encription Protocols, Public Keys Algorithms, and Digital Signatures
Academic Press
1985.

Garfinkel, S. y Spafford, G.
Web and Security Commerce
O'Reilly Associates, Inc.
1997.