INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS DE LA DIVISIÓN DE ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

SEGURIDAD EN REDES Y CRIPTOGRAFÍA

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADÉMICO DE: MAESTRO EN CIENCIAS CON ESPECIALIDAD EN INGENIERÍA ELECTRÓNICA (TELECOMUNICACIONES)

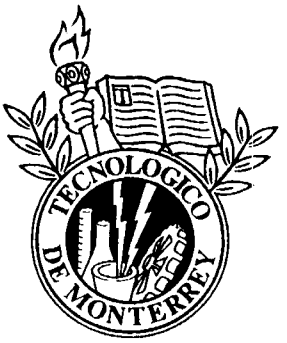
DANTE IVÁN GONZÁLEZ SÁNCHEZ

ENERO DE 2004

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS DE LA DIVISIÓN DE ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES



SEGURIDAD EN REDES Y CRIPTOGRAFÍA

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADÉMICO DE: MAESTRO EN CIENCIAS CON ESPECIALIDAD EN INGENIERÍA ELECTRÓNICA (TELECOMUNICACIONES)

DANTE IVÁN GONZÁLEZ SÁNCHEZ

ENERO DE 2004

SEGURIDAD EN REDES Y CRIPTOGRAFÍA

TESIS

MAESTRÍA EN CIENCIAS CON ESPECIALIDAD EN INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

POR

DANTE IVÁN GONZÁLEZ SÁNCHEZ

ENERO DE 2004

DEDICATORIA

Para mi familia, ellos fueron la fuerza impulsora en los momentos difíciles y sin su apoyo esta aventura jamás habría sido posible.

ÍNDICE

ABSTRACT

El presente es una investigación referente al problema que existe de seguridad en redes e Internet. Se hace un recuento de las técnicas, problemas y principales conceptos de seguridad computacional para proveer un panorama claro de la situación actual, y se plantean soluciones para el mejoramiento e implementación de la seguridad en distintos tipos de redes con conexión y sin conexión a Internet. Se presentan los resultados de comparar el algoritmo de encripción de llave privada implementado en MAPLE basado en DES, un algoritmo Blowfish, un algoritmo de uso exclusivo de CES Encryption Utility, y un algoritmo de llave pública implementado en MAPLE basado en el RSA. Se muestran los resultados obtenidos en cuanto a los tiempos de transferencia de archivos encriptados en una red, se comparan los tiempos de procesamiento de la encripción con llave pública y con llave privada. Con la información obtenida y según las necesidades personales se tienen los medios para tomar la decisión más acertada sobre el tipo de encripción o programa que más conviene. Con esto se espera otorgar suficientes datos para quien desee conocer como protegerse de incursiones no deseadas en sus sistemas de computadoras.

OBJETIVO

Uno de los objetivos de la investigación es lograr proponer varias soluciones informáticas por medio de encripción, políticas, técnicas y herramientas para así elevar la seguridad en varias configuraciones de sistemas de cómputo. Proporcionando así, una guía con la información necesaria para poder asegurar los datos contenidos en un sistema y la transferencia de estos; presentando de manera clara las configuraciones más usuales de sistemas de computo, sus vulnerabilidades y posibles soluciones.

Otro de los objetivos de la investigación es hacer una comparación de los tiempos de procesamiento del algoritmo simétrico Blowfish, el algoritmo simétrico DES y del algoritmo asimétrico RSA. También se compararon los tiempos de transferencia de archivos encriptados desde una computadora a otra, la encripción de estos archivos fue realizada con programas que utilizan algoritmos de llave privada -el programa Advanced Encryption Package utilizando el algoritmo simétrico Blowfish; el programa CS Enigma utilizando el Blowfish, el programa Crypto con el algoritmo Blowfish, el programa CES Encryption Utility con un algoritmo de uso exclusivo-, un algoritmo de llave pública implementado en MAPLE basado en el RSA y un algoritmo de llave privada implementado en MAPLE basado en DES. Con estas comparaciones se quiere corroborar de manera experimental que una encripción asimétrica exige más recursos del sistema que una encripción simétrica, y observar si la transferencia de un archivo encriptado es distinta a la transferencia de un archivo normal y que tanto influye en la red el cambio de tamaño por encripción. Con estos datos, se pueden analizar los beneficios que nos otorgan cierto método de encripción, y saber al mismo tiempo, si ese método de encripción no afectara la transferencia en la red o el rendimiento del sistema, ya que, se puede presentar el caso de que la encripción es resistente a numerosos tipos de ataques pero exige mucho tiempo de procesamiento y recursos, además puede aumentar demasiado el tamaño del archivo causando que la transferencia se vuelva mas lenta. Para algunos usuarios los retardos y consumo de recursos pueden no ser importantes con tal de obtener una encripción resistente, pero para otros la velocidad de encripción y transferencia es más importante que la resistencia a los ataques.

JUSTIFICACIÓN

La investigación que se hará en el campo de la computación y redes será de gran ayuda para un enorme número de usuarios que utilizan Internet para realizar transacciones. Los beneficiarios de tener una red más segura van desde el simple estudiante hasta las grandes corporaciones. Cada uno de los usuarios de sistemas computacionales tendrá necesidades diversas, por esto, se presentaran aquí una recopilación de distintas configuraciones de sistemas computacionales, métodos y herramientas para mantener la seguridad de la información. Con esto, se quiere mostrar un panorama más amplio de lo que significa tener privacidad de archivos importantes y ante la gran cantidad de programas que se pueden encontrar en Internet y a la venta, poder presentar los más usuales o de fácil acceso y al definir sus características permitir a los interesados decidir cuales son los más efectivos para la configuración del sistema computacional que se tenga, de manera que al mismo tiempo en que se logra un buen nivel de seguridad no se afecte demasiado la transmisión por la red o el rendimiento del sistema. Se harán pruebas para observar el comportamiento de un algoritmo de llave pública contra algoritmos de llave privada, y ver sus posibles aplicaciones en negocios donde se requiera la transmisión de texto o de algunos símbolos; los programas que generaran los archivos encriptados por medio de una llave privada son encontrados en Internet y se escogió utilizarlos por la facilidad con que se obtienen, así que es probable que los usuarios de equipo de computo que necesiten de privacidad en sus archivos probablemente busque utilizar estos o ya los estén utilizando. Al tener un programa o algoritmo que se encargue de mandar de manera segura nuestra información, seguramente se presentará un incremento en las personas que utilicen las compras por Internet, la transferencia de dinero y la utilización de los números de tarjetas de crédito sin ningún problema. Muchas de estas transferencias son entre dos computadoras, por ello, las pruebas se harán también entre dos computadoras para poder apreciar cual es la exigencia sobre la red en cuanto a la transferencia de archivos encriptados. Los parámetros que se evalúan con la finalidad de poder apreciar si la encripción con cierto algoritmo realmente es conveniente son: tiempo de transmisión de archivos encriptados, tiempo de procesamiento para la encripción de archivos, observando además si en que porcentaje el tamaño del archivo aumenta o disminuye y la información de los paquetes para observar su comportamiento en caso de perdidas de paquetes. Al tener estos datos, se verán cuales son las características de velocidad y seguridad que cada algoritmo ofrece, esto es muy útil porque permite apreciar las ventajas y desventajas de los algoritmos de encripción analizados aquí. Para ciertos usuarios las características de mayor resistencia a ataques en un archivo encriptado son más importantes, mientras que para otros lo importante es tener una red con una velocidad de transferencia constantemente buena y utilizar un algoritmo que otorgue cierta seguridad sin requerir demasiados recursos del sistema para la encripción. Así, los usuarios decidirán cuál aplicar en su sistema según sus preferencias y necesidades.

Al lograr un buen nivel de seguridad computacional se puede incrementar el número de negocios electrónicos o para algunas empresas que ya están establecidas cabe la posibilidad de que abran nuevas ramas de servicios en línea.

INTRODUCCIÓN

A través de los años las necesidades de seguridad han ido cambiando, ya que antes del advenimiento de las computadoras y de la era de la información digital, los documentos y la información que se denominaba como confidencial se guardaban solo en archiveros especiales y se ponían bajo llave. Es decir que para la época en que la información era primordialmente física, también se utilizaban medios físicos para su privacidad.

El amplio desarrollo que ha tenido la cultura informática ha propiciado el hecho de que, al igual que en nuestra cultura social, aparezcan individuos con tendencias delictivas ignorantes de las leyes ya establecidas por la comunidad informática, tanto en Internet como en las redes locales de oficinas y negocios. Como respuesta a las crecientes amenazas en el mundo informático, se han promulgado leyes en los sistemas judiciales para tipificar los delitos computacionales en muchos países, e incluso con penas de varios años de cárcel dependiendo del monto de información robada. Al mismo tiempo, los fabricantes de equipo de conectividad y diseñadores de software se han dedicado al desarrollo de nuevas tecnologías en software y hardware para proteger las redes y mantenerlas en monitoreo constante, también han diseñado aparatos para rastrear a los atacantes que provienen desde una red externa. Esto ha propiciado la aparición de equipos de trabajo dedicados a la protección, análisis de vulnerabilidades y creación de herramientas que permitan su aplicación en un sistema y así, una mejor sensación de seguridad.

Sin embargo, toda la información en cuanto a seguridad puede resultar en cierto momento "asfixiante". Entre algoritmos de encripción simétricos y asimétricos, funciones Hash, protocolos de seguridad, protocolos de comunicación, actualizaciones de sistemas, antivirus, detectores de intrusos, firewalls, analizadores de tráfico y programas de auditorias existen demasiados programas y métodos que permiten aplicar cierto nivel de seguridad a los sistemas, de manera que un usuario con conocimientos básicos de conectividad y computación que desee tener un nivel dado de seguridad, tendría que pasar mucho tiempo investigando que tipo de software y hardware serán los mas útiles para su configuración de sistema en particular.

Es por ello que la intención de este documento de seguridad en redes y criptografía es poder dar una mejor visión acerca de las tecnologías para la protección de los sistemas de computación. En el primer capitulo del documento se presentan los aspectos generales de la seguridad informática, conceptos, amenazas, tipos de ataques informáticos, herramientas de atacantes, niveles de seguridad y algunos casos muy conocidos de ataques informáticos.

En el segundo capitulo se analizan los mecanismos de seguridad con que hacer frente a las amenazas de ataques y robos de información, principalmente la criptografía y los distintos tipos de algoritmos y funciones Hash.

Para el tercer capitulo se presentan los protocolos de seguridad que se utilizan hoy en día para las transferencias y la comunicación segura por Internet. Aquí se incluye el protocolo IPv6 por las nuevas características de seguridad con las que cuenta en sus encabezados de paquete (*headers*) y que ya es soportado por varios sistemas operativos y en algunas redes con conexión a Internet ya esta siendo aplicado.

En el cuarto capitulo se hacen recomendaciones de seguridad en las áreas de criptografía, controles de software, controles de hardware, controles físicos y políticas para varias configuraciones de sistemas informáticos. Aquí se incluyen las configuraciones más populares, redes con conexión a Internet y similares. Al final se le otorga un nivel de seguridad a cada configuración.

Para el quinto capitulo se presentan los resultados de las pruebas de encripción y transferencia de archivos. La encripción se llevo a cabo con algoritmos desarrollados en MAPLE y con programas de encripción de llave privada.

Para finalizar el documento se presenta un capitulo con las conclusiones obtenidas respecto a la seguridad de las configuraciones y el comportamiento de los algoritmos utilizados en las pruebas.

La seguridad informática se esta volviendo un tema cada vez mas conocido, muchas veces son exageradamente publicitados los casos de gusanos informáticos (*worms*) que causan la caída de sistemas. Es claro que conforme la tecnología llega a un mayor número de individuos, los afectados por los problemas de los sistemas aumentaran. La mayoría de las personas no ponen atención en esta clase de cosas, pero parte de la solución recae en que nosotros, como usuarios, hagamos conciencia de que utilizar la computadora de cierta manera puede ser insegura, y que debemos apegarnos a las recomendaciones de seguridad para sacar el mejor provecho de las posibilidades de comunicación ofrecidas por las redes.

CAPITULO 1

ASPECTOS GENERALES DE LOS PROBLEMAS EN LA SEGURIDAD

Características de Intrusión Computacional.

Un sistema computacional lo definimos como una colección de hardware, software, medio de almacenamiento y también la gente que se encarga del manejo de las tareas computacionales. En una intrusión a un sistema los blancos pueden ser diversos: una lista de clientes, direcciones, cuentas, etc. Esto hace que la seguridad en computacional sea más complicada debido a la variedad de blancos. En un sistema de seguridad, se puede decir que la resistencia del sistema depende de su parte más débil.

Conceptos Importantes de seguridad

- **Exposición**: Es una forma de posible pérdida o daño en un sistema computacional, por ejemplo el acceso no autorizado de información, la modificación de información, o la negación de acceso a un servicio.
- **Vulnerabilidad**: Es una debilidad en el sistema que puede ser explotada para causar pérdida o daño. Si una persona explota una vulnerabilidad se está perpetrando un ataque al sistema.
- **Amenazas**: Son circunstancias que tienen el potencial de causar pérdida o daño, los ataques humanos son ejemplos de amenaza, al igual que los desastres naturales, errores inadvertidos, etc.
- **Control**: Es una medida de protección que reduce una vulnerabilidad.
- **Amenazas contra Hardware**: Estos se refieren a ataques físicos contra el equipo de computo, tal como prenderles fuego, lanzarles agua, roedores, llaves y desarmadores que causan corto circuitos.
- **Amenazas contra Software**: El software puede ser destruido maliciosamente, modificado, borrado o colocado erróneamente. Estos errores se presentan cuando uno trata de acceder al software.
- **Amenazas contra Datos**: Los datos son especialmente vulnerables a la modificación. Ya que si está es hecha de manera habilidosa no será detectada.

Los ataques pueden ser de diferentes tipos, un ejemplo clásico de estos ataques es la utilización de los "virus de computadoras", como seguramente ya muchos hemos experimentado, los virus pueden ser enormemente molestos y peligrosos para cualquier usuario que no este debidamente protegido contra ellos. Existe una enorme cantidad de virus hoy en día, aunque afortunadamente también existe una buena cantidad de programas antivirus que nos permiten deshacernos de ellos. Un virus puede llegar a nuestra computadora por medio de un disco contaminado o a través de la red y sus efectos pueden ser variados, van desde el simple reacomodo de información, hasta la destrucción de datos específicos o de archivos propios del sistema.

La seguridad de los sistemas de información esta amenazada por un número creciente de problemas, ya que no solo de los virus tiene uno que proteger los archivos. Veamos algunos de los ejemplos que pueden darse en donde la seguridad es violada:

1. El usuario ***A*** transmite un archivo al usuario ***B***. Si este archivo contiene información delicada (por ejemplo los registros de la nomina de pagos) que necesita ser protegida del conocimiento público. Un usuario ***C***, quien no tiene autorización para leer este archivo, puede monitorear esta transmisión y obtener una copia del archivo durante la transmisión.
2. Un administrador de red ***X***, transmite un mensaje a la computadora ***Y***, la cual esta bajo su administración. Si, por ejemplo, este archivo es una actualización de un archivo de autorización que incluya a los nuevos empleados que tienen acceso a esta computadora y un usuario ***F*** intercepta el mensaje, altera su contenido borrando o agregando registros y posteriormente mandarle el archivo modificado a la computadora ***Y*** la cual lo acepta como si este viniera del administrador ***X***.
3. La misma situación antes mencionada pero si ahora el usuario ***F*** en lugar de interceptar el mensaje crea su propio archivo y lo envía a la computadora ***Y*** como si este procediera del administrador ***X***.
4. Suponiendo que un empleado sea despedido sin advertencia, el administrador de personal le envía un mensaje al servidor para que invalide las cuentas de este empleado, el servidor entonces manda una confirmación al archivo del empleado para confirmar la acción. Si el empleado tiene los medios necesarios para retrasar este mensaje, él puede hacer una última incursión en el servidor y así obtener información confidencial. Después de esto el empleado deja que el mensaje continué y esta acción puede pasar desapercibida por mucho tiempo.

El último ejemplo que se menciona es el medio más común por el cual suceden robos de información. Muchos de los negocios hoy en día solo están contratando personal de manera temporal y si a uno de estos empleados se le ofrece una plaza permanente en otra compañía competidora, esta persona podría llevarse información muy importante a la que tiene acceso antes de retirarse, lo cuál le puede asegurar un rápido ascenso en su nuevo lugar de trabajo. Un estudio realizado en 1996 y 1999 cuya información completa se encuentra en el *FBI/CSI Computer Crime & Security Survey, 1999* nos muestra que en 1999 del total de los negocios que sufrieron ataques y robo de información en el 55% de los casos esto fue hecho por gente dentro de la red o del sistema. [1]

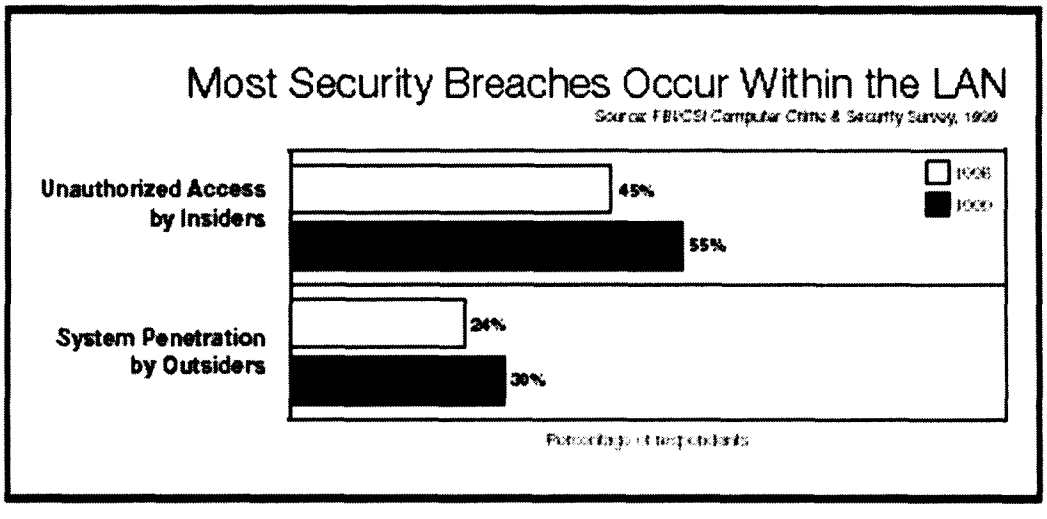


Figura 1.1 - Gráfica de los principales culpables de ataques en una red local

ATAQUES, Y MECANISMOS PARA IDENTIFICARLOS

Para asegurar la correcta utilización de los sistemas de seguridad se han considerado tres aspectos de la seguridad informática:

- **Ataque a la seguridad**. Esto es cualquier acción que comprometa la seguridad de la información que tiene cualquier organización.
- **Mecanismos de seguridad**. Un mecanismo que está diseñado para detectar, prevenir o recuperar a la seguridad de un ataque.
- **Servicio de seguridad**. Un servicio que mejora la seguridad de los sistemas de procesamiento de datos y las transferencias de información de una organización. Los servicios están hechos con la intención de contrarrestar ataques a la seguridad, y hacen uso de uno o más mecanismos de seguridad para proveer el servicio.

Veamos ahora cada parte de estos aspectos por separado:

ATAQUES

G.J. Simón menciona muy apropiadamente que la seguridad informática se basa en prevenir las trampas y trucos que permiten el acceso sin autorización, y que en dado caso de que se falle en prevenirlos, ser capaces de detectar estas trampas y trucos en los sistemas donde la información se ha visto afectada.

Hay diversas razones para crear problemas de este tipo, por ejemplo, para ganar acceso a información no autorizada, hacer una fraudulenta atribución de la responsabilidad si se accesa a información clasificada, incrementar las licencias con las que se cuenta actualmente y así tener acceso a más datos reservados, incorporarse uno mismo a un enlace de transmisión entre otros usuarios como un punto de retransmisión activo e indetectable, causar que otros violen un protocolo mandando o introduciendo información incorrecta, minimizar la confianza en un protocolo causando aparentes falla en el sistema, aprender quien accesa cierto tipo de información y cuando son hechos estos accesos, prevenir la comunicación entre otros usuarios causando interferencia que haga creer que información autentica sea rechazada por parecer que no lo es, etc.

Diversos estudios se han realizado para determinar las características de las personas que cometen el crimen computacional, estos estudios son con la intención de que las compañías detecten a los probables criminales y prevengan el crimen: **Amateurs, Crackers y los criminales de carrera**.

Amateurs: La mayor parte de los crímenes cometidos hasta la fecha son por amateurs. No son criminales de carrera sino gente normal que observan una falla en el sistema de seguridad que les permite el acceso a dinero u otros valores. Las situaciones de ataques pueden iniciarse cuando este empleado descubre una falla o quiere aprovecharse de ella, o en algunos casos vengarse de sus jefes o compañeros de trabajo.

Crackers: Estos pueden ser estudiantes de colegio o preparatoria quienes intentan acceder instalaciones de computadoras para las cuales no tienen autorización. Romper las defensas de computadoras es visto como el máximo crimen sin victima. No se lastima a nadie o se le pone en peligro. La mayor parte de la incursión puede llevarse a cabo sin confrontar a nadie. Debido a esta ausencia de reprimendas o prohibición de acceso, el cracker asume que no hace nada indebido. Algunos crackers causan ataques para lograr un éxito mayor junto con otros crackers o simplemente para ganar respeto o satisfacción propia y algunos solo quieren causar

caos, pérdida o daño. Esta tendencia ha causado pérdidas de varios millones de dólares en daños y aunque se han impuesto duras penas a los que cometen este tipo de crímenes sigue siendo muy atrayente para los jóvenes.

Criminales de carrera: El criminal de carrera entiende perfectamente las metas del crimen computacional. Los criminales generalmente inician como profesionales de computación quienes se enredan en el crimen y encuentran que los resultados son muy buenos. Existe evidencia que grupos del crimen organizado se están interesando cada vez mas por el crimen computacional. Los espías electrónicos han reconocido que intercambiar secretos de compañías puede ser muy lucrativo. Muchas veces las compañías no inician acción legal contra el criminal computacional, las compañías prefieren dejar de usar el sistema cuya seguridad fue comprometida en lugar de reunir evidencia que permita detener al atacante, lo cual permite que el criminal siga libre y emplee los mismos patrones ilegales contra otra compañía.

ATAQUES A LA SEGURIDAD

Si vemos a un sistema de computadora o a una red como un proveedor de información, los ataques pueden caracterizarse. En general existe un flujo de información desde una fuente, tal como un archivo o una región de memoria principal, hacia un destino, que puede ser otro archivo o usuario. Este flujo normal se muestra a continuación en la figura 1.2:

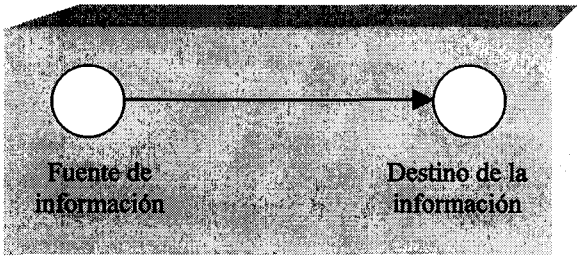


Figura 1.2 - Flujo normal de datos

A continuación mencionaremos las cuatro categorías generales de los ataques:

- **Interrupción.** Una de las capacidades del sistema es destruida o se vuelve inaccesible o no usable, este es un ataque sobre la disponibilidad. Ejemplos de esto incluyen la destrucción de una pieza del hardware, tal como el disco duro, el corte de una línea de comunicación, o deshabilitar el sistema administrador de archivos.

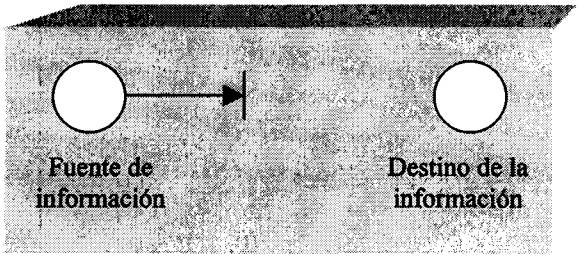


Figura 1.3 - Interrupción

- **Intercepción.** Un equipo no autorizado gana acceso a una característica. Este es un ataque sobre la confiabilidad. Ejemplos de esto pueden ser el agregado de alambres en una red para capturar información, y la copia ilícita de archivos o programas.

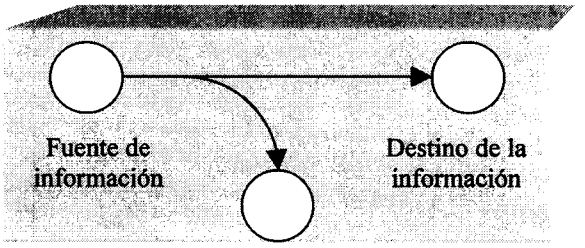


Figura 1.4 - Intercepción

- **Modificación.** Un equipo no autorizado no solo gana acceso, sino que modifica una característica. Este es un ataque sobre la integridad. Ejemplos de esto incluyen el cambiar valores en un archivo de datos, alterando un programa para que se desempeñe de manera diferente, modificar el contenido de mensajes que están siendo transmitidos por una red.

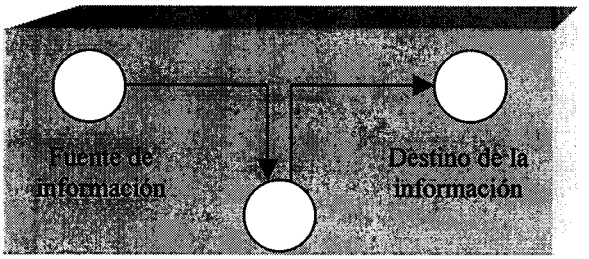


Figura 1.5 - Modificación

- **Fabricación.** Un equipo no autorizado inserta objetos distractores dentro del sistema. Este es un ataque a la autenticidad. Ejemplos incluyen la inserción de archivos imitadores en la red o la adición de registros a un archivo.

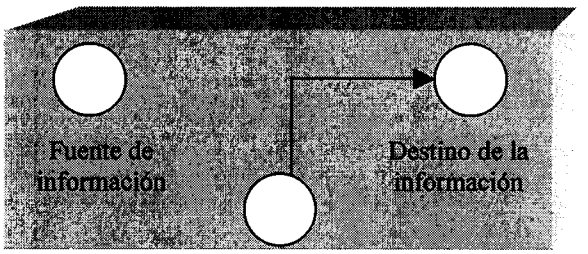


Figura 1.6 - Fabricación

W. Stallings nos dice que una categorización útil de estos ataques sería en términos de ataques activos y ataques pasivos.[2, capitulo 1]

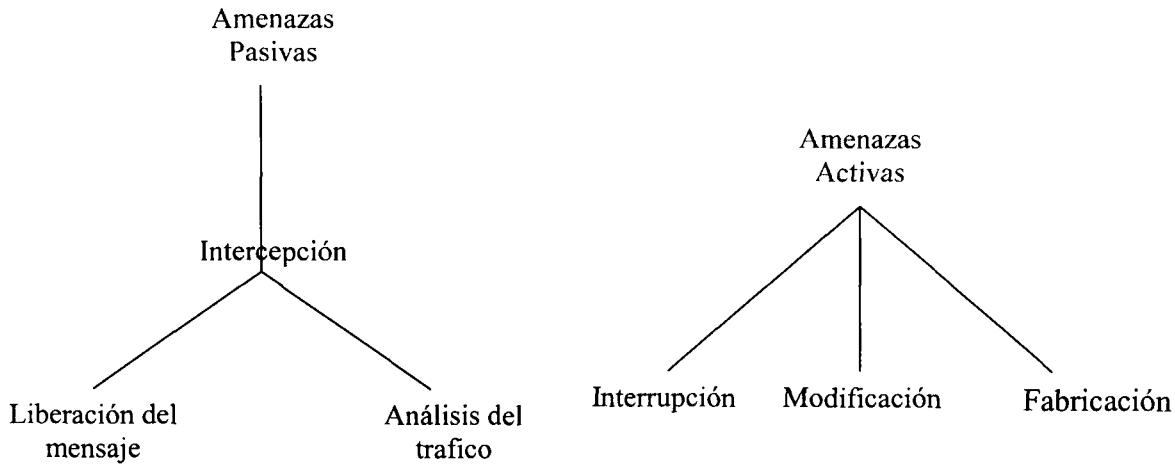


Figura 1.7 - Categorización de ataques

Para estos ataques se utilizan diversos tipos de herramientas, algunos son comandos, otros son programas, veamos cuales son y sus aplicaciones:

Comandos de usuario.- Estos son introducidos por medio del teclado, estos comandos le permiten al atacante introducirse a una cuenta ajena y modificar o borrar información.

Script o Programa.- Los scripts son una serie de comandos, con los que se produce la interrupción, intercepción o modificación. Ejemplos de estos son los programas conocidos como *cracks*.

Agentes Autónomos.- Estos son programas colocados dentro de los sistemas y que eligen su blanco. Los virus y los gusanos (worms) son los clásicos ejemplos de estos agentes.

Toolkits.- Estos son paquetes de herramientas que son usados por los atacantes para efectuar la modificación, intercepción o interrupción. Algunos de estos paquetes contienen programas del tipo Caballo de Troya (*trojan horse*), los cuales esconden su actividad y pueden crear puertas traseras (*backdoors*) para facilitar una nueva entrada al sistema tiempo después.

Herramientas distribuidas.- La función de estas herramientas consiste en que una vez que hayan sido colocadas dentro del sistema blanco, esperan una señal o un tiempo para activarse y causar un sobre flujo de información en este sistema y así causar su caída e imposibilitar a otros usuarios su utilización. Esto ha ocurrido muy frecuentemente en numerosas páginas web.

Debido a la gran cantidad de herramientas y técnicas que se han venido desarrollando en los últimos años, el número de ataques dentro del ámbito informático se ha ido incrementando en gran medida. Aunado a esto, tenemos que los precios de equipo de computo cada vez más poderoso se han vuelto más accesible y mucha de la información concerniente a como explotar vulnerabilidades y deficiencias en la protección de computadoras es compartida en páginas de Internet y en salones de conversación virtuales. Gente alrededor del mundo con los conocimientos necesarios, poca ética profesional y sombríos intereses son los encargados de aprovechar las facilidades de la era de información; también están los usuarios demasiado jóvenes que sienten la necesidad de probar sus habilidades contra las capacidades de un sistema supuestamente protegido. Para ejemplificar de mejor manera todo, se presentan a continuación una serie de casos reales y bastante publicitados en donde se puede ver de una manera real las consecuencias de un

ataque a una red de computadoras, y lo critico que puede llegar a ser la ruptura de la seguridad en un sistema:

- **CASO 1**. El 2 de Noviembre de 1988 fue liberado en Internet un gusano, causando grandes estragos en diversos equipos. El gusano fue creado y liberado por Robert T. Morris Jr., quien lo programó para que determinara donde se podía esparcir, diseminara la infección y que al final se ocultara.
  Las consecuencias de la diseminación de este gusano fueron varias, causo el agotamiento de recursos en las maquinas afectadas, esto fue porque el código del gusano revisaba si otras máquinas ya habían sido infectadas, pero debido a un error de programación algunas computadoras contenían múltiples copias del gusano intentando diseminar la infección. En tales computadoras los administradores debieron cortar su conexión a Internet para evitar ser infectados y detener el proceso de infección hacia otros lugares. Al verse obligados los administradores a cortar la conexión de estos equipos y sistemas, las tareas de comunicación, investigación, colaboración e intercambio de información no pudieron seguirse realizando; por lo que diversos sistemas y redes de una misma empresa quedaron aisladas de sus contrapartes en otros lugares.
  El código del gusano explotaba varias vulnerabilidades conocidas y fallas de configuración en la versión 4 Berkeley del sistema operativo UNIX. Para definir donde esparcirse, el gusano intentaba aprovechar el hecho de que los archivos de passwords en UNIX son encriptados pero se puede ver el texto cifrado y así, encontrar cuentas de usuarios del equipo atacado, paralelamente trataba de explotar un error de programación (*bug*) en el programa ***finger*** donde causaba un sobreflujo en el buffer de entrada haciendo que se desbordara hacia la pila de dirección de retorno, después de esto usaba una puerta trampa (*trapdoor*) en el controlador de correo ***sendmail*** donde se le enviaba una señal para que reciba correo pero en modo ***debug,*** así el programa recibe y ejecuta una cadena de comandos en lugar de la dirección destino. Si el gusano encontraba una computadora propicia para esparcirse, el gusano utilizaba uno de los métodos anteriores para enviar a la máquina atacada un cargador ***bootstrap***, el cual consistía de 99 líneas de código en C compiladas y ejecutadas por la computadora atacada. El cargador de ***bootstrap*** pedía el resto del código del gusano a la máquina de origen. El ***bootstrap*** se encargaba de no dejar huellas, ya que si ocurría un error de transmisión cuando se enviaba el resto del código, el cargador se ponía en cero y borraba todo el código ya transferido. Una vez que el gusano se encontraba bien establecido en un anfitrión hacia todo lo posible para evitar ser descubierto, tan pronto como el gusano reunía todo su código en una nueva máquina lo mandaba a memoria, lo encriptaba y borraba las copias originales del disco. Por lo que no había rastro en disco, y una revisión de memoria no expondría inmediatamente el código del gusano, posteriormente el gusano cambiaba periódicamente su nombre e identificador de proceso para que no corriera mucho tiempo con un solo nombre.
  El gusano causo que 6000 instalaciones se apagaran o desconectaran de Internet, el costo de los daños fueron desde $100,000 hasta $97 millones de dólares. **[32, capitulo 5]**

- **CASO 2**. En febrero de 1998 los sistemas de computadoras del Pentágono sufrieron un ataque causado por dos piratas adolescentes del estado de California. El edificio del Pentágono es conocido como el centro de la inteligencia militar de los Estados Unidos y en cuyas bases de datos se contiene la información de diversas actividades llevadas a cabo por este gobierno alrededor del mundo, así como los proyectos secretos y operaciones militares, presumiblemente el lugar con la información más secreta y mejor resguardada del mundo. Según los reportes dados a conocer, en este ataque no se puso en riesgo información de la seguridad nacional de los Estados Unidos, sin embargo sirvió para demostrar una vulnerabilidad que podría haber resultado en pérdidas desastrosas de información en el futuro. En el Pentágono y otros edificios del gobierno de Estados Unidos

la información más delicada se protege por medio de un muro de aire, es decir que esta información no se puede accesar desde una red externa.[3]

- **CASO 3**. El 17 de Marzo de 1998 la red de computadoras de la Universidad de Minnesota en los Estados Unidos, sufrió un ataque del tipo de "negación de servicios" el cual causó pérdida de información y un alentamiento en la conexión a Internet en todo el estado de Minnesota. El ataque fue perpetrado a las 11 a.m. y tuvo una duración de más de una hora, según fuentes de la Universidad, aunque otros sitios afectados declararon haberlo sentido desde más temprano y por más tiempo.
  Este ataque dirigido a la Universidad causó una reacción en cadena en todo el estado apagando algunas computadoras completamente y en otros casos hubo pérdida de información y alentamiento en la red. Se podría decir que causo un "embotellamiento del trafico" en la red, según palabras de Susan Levy-Haskell, coordinadora de respuesta a incidentes de seguridad de la Universidad de Minnesota. Ella misma indica que fue necesario quitar la conexión al Campus Crookston de la Universidad, el blanco del ataque.
  La compañía MRNet, la organización de servicio de Internet más grande en Minnesota, declaro que tuvieron cerca de dos horas y media con un servicio severamente degradado con un 30% en pérdida de paquetes. MRNet definió el ataque como del tipo negación de servicio "pitufo" (*smurf*). En estos ataques se envían paquetes de "ping" para pedir respuesta de computadoras en red. En un ataque "pitufo", el atacante especifica la computadora objetivo del ataque como la dirección de retorno de los paquetes ping y envía suficientes peticiones para garantizar una enorme cantidad de respuestas. Este ataque sobre la Universidad afecto a MRNet porque el proveedor tiene un acuerdo cooperativo con la Universidad para compartir el ancho de banda provisto por las empresas MCI *Communications* y *Sprint*. Las *compañías Fortune 500, algunos negocios pequeños* y casi todos lo colegios privados del estado de Minnesota también sufrieron las consecuencias por ser clientes de MRNet.
  Apenas una semana antes, el 2 de Marzo la Universidad de Minnesota fue también blanco de ataques de negación de servicio, al igual que las redes de la NASA, la Marina y de diversos campus universitarios en todo Estados Unidos. [4]

- **CASO 4**. El 27 de Mayo de 1999 el sitio en Internet de la Agencia Federal de Investigación de los Estados Unidos (FBI) fue atacado. Este ataque no tuvo éxito, sin embargo el FBI tuvo que quitar de la red el sitio para aislar el intento de intrusión. Este intento fue como respuesta a la persecución de piratas computacionales un día antes por el FBI.
  Uno de los piratas, quien se hace llamar Israelí Ghost, protestó a esta persecución con un ataque de negación de servicio inundando la conexión con información de manera que el sitio no pueda trabajar. Más tarde, otros piratas modificaron las páginas de algunos sitios adicionales en Internet. [5]

- **CASO 5**. Los ataques sobre los sitios de Yahoo, eBay, Buy.com, CNN.com y Amazon comenzaron el 7 de febrero de 2000, poco después, el 9 de febrero los sitios de las compañías ZDNet y de E-Trade también fueron atacados. El ataque fue del tipo de negación de servicio (*denial of service*) el cual no implica el introducirse al sitio sino simplemente sobrecargarlo, haciendo que los ruteadores que conectan los sitios se inunden con demasiado tráfico falso el cual ya no es capaz de ser manejado. Una vez logrado esto y que el sitio esta sobrecargado, los usuarios genuinos encuentran que no pueden acceder al sitio.
  Estos ataques fueron preparados desde hace tiempo al plantar el software necesario en muchas computadoras de la red, principalmente en las redes de universidades y después solo fue cuestión de dar la orden de iniciar el ataque.

El primero en sufrir el ataque fue el sitio Buy.com quien tuvo su red virtualmente inaccesible unas horas después de que el sitio había completado una oferta pública inicial. Aproximadamente a las 10:50 a.m. del 7 de febrero, el sitio experimentó el alentamiento por el ataque de negación de servicio, 800 megabits de información por segundo llegaban al sitio, que es ocho veces la capacidad máxima que puede manejar Buy.com.
Más tarde, a las 3 p.m. el sitio de eBay experimentó un ataque de negación de servicio. Este fue más largo ya que continuó hasta el 8 de febrero. El ataque afectó sus servidores en el centro de datos de AboveNet Communications. Estos servidores cargan las páginas estáticas de eBay, tales como su página principal o la del perfil de la compañía. Las páginas dinámicas que se encargan de las subastas, el listado y búsqueda son manejadas por una compañía distinta y por lo tanto no fueron afectadas, por eso eBay aseguro que la mayor parte de su sitio estaba funcionando siempre y cuando los usuarios tuvieran grabadas las direcciones de otras páginas en el sitio que no fuera la página principal.
El famoso sitio de ventas Amazon.com fue atacado a las 5 p.m. del 7 de febrero, también por negación de servicio. Una enorme cantidad de tráfico basura fue enviada al sitio de Amazon con lo que se degrado el servicio durante una hora.
CNN.com también fue atacado en el mismo momento que Amazon, el rendimiento en el sitio de CNN normalmente es del 95% y cayo hasta el 18% en el periodo de 4 p.m. a 4:15 p.m. y más tarde cayó hasta un rendimiento de cero entre las 5 p.m. y 5:15 p.m. de acuerdo a datos dados por Keynote Systems compañía dedicada a medir el rendimiento en Internet. [7][8]

- **CASO 6**. En julio del 2001 un gusano (*worm*) infectó cientos de miles de servidores de Internet alrededor del mundo en menos de una hora. Los investigadores de la Asociación Cooperativa para el Análisis de Datos de Internet (CAIDA) utilizaron técnicas de análisis "*backscatter*" (desarrolladas para detectar ataques de negación de servicio) para rastrear el progreso de la infestación.
  En esa ocasión más de 359,000 computadoras fueron infectadas con una versión del gusano "Code Red", incluso durante el momento pico de la infestación más de 2000 nuevas maquinas eran infectadas cada minuto. Code Red infecta servidores de Internet explotando una vulnerabilidad en el paquete de software de Microsoft, de Servicios de Información de Internet (IIS), por tanto Code Red solo afecta sistemas que corren software de Microsoft. El 12 de julio, menos de un mes después de que la vulnerabilidad en IIS había sido dada a conocer a la comunidad dedicada a la seguridad, el gusano Code Red fue detectado por Marc Maiffret y Ryan Permeh de eEye Digital Security. Poco después, el 19 de julio una nueva y mejorada versión del gusano apareció. Una vez que infecta un anfitrión, Code Red intenta esparcir la infección enviando una copia de sí mismo a 99 direcciones de IP aleatorias. Y después espera. El día 20 del mes, cada copia de este gusano ataca el sitio de la Casa Blanca en los Estado Unidos con mensajes intentando sobrecargar su servidor de Internet. El administrador de red de la Casa Blanca fue alertado del problema y cambio la dirección numérica de IP del servidor, lo que previno la fase de ataque de Code Red.
  De las máquinas infectadas, el 43 por ciento de ellas fueron en los Estados Unidos, el 11 por ciento en Corea, 5 por ciento en China, y un 4 por ciento en Taiwán. Los sitios que tuvieron más máquinas infectadas fueron los de dominio ***.NET*** con un 19 por ciento del total, seguidas por ***.COM*** con 14 por ciento y ***.EDU*** con 2 por ciento. El gusano Code Red fue programado para un causar un máximo de molestias pero un mínimo de daño, ya que no altera los archivos en el disco duro y reside solo en memoria, pueden deshacerse del gusano con un reinicio de la computadora. [10]

- **CASO 7**. A principios del año 2003 el tráfico mundial de Internet sufrió el ataque del gusano (*worm*) SQL Slammer, el cual estuvo a punto de evitar accesos a la red en Corea del Sur y detuvo muchos cajeros automáticos en los Estados Unidos.

Este se considera como el primer gusano del tipo flash, un programa de ataque que se propaga tan rápidamente que no se puede responder lo suficientemente rápido. SQL Slammer explotó una vulnerabilidad previamente conocida en las bases de datos corporativas SQL de Microsoft que no tenían instalado un parche que apareció seis meses antes. SQL Slammer infectó 200,000 computadoras y se esparció al 90% de ellas en los primeros 10 minutos de haber aparecido en Internet. [11][12]

- **CASO 8**. El sitio de la Asociación de América de la Industria de Grabación, RIAA.org fue atacado el 7 de febrero de 2003 y sacado de línea. Este ataque fue el último registrado de una serie de asaltos en el sitio de la industria musical, aparentemente como retribución por la desaparición del software que permite traspasar archivos de terminal a terminal, propiciado por la RIAA.
  RIAA, que representa a las más grandes compañías de grabación musical, ha tenido su sitio de Internet continuamente fuera de línea como resultado de ataques de piratas. No solo han sacado de la red el sitio sino que también le han hecho modificaciones al sitio agregando links a páginas de descargas ilegales de música. Un mes antes el sitio también había sido atacado bloqueando accesos al menos durante tres días.
  Después de este ataque RIAA decidió cambiarse al proveedor TST lo cual se podría ver como un movimiento inteligente ya que la compañía anfitriona se encontraba ofreciendo un programa de investigación de crímenes de alta tecnología para agencias federales, estatales y locales en los Estados Unidos. Sin embargo, levantó muchas dudas el hecho de que un proveedor que ofrece entrenar oficiales de la ley no pueda mantener seguro contra ataques el sitio de uno de sus clientes. [13]

- **CASO 9**. El 10 de Marzo de 2003 se registró un ataque en un servidor del Ejercito de los Estados Unidos, explotando una vulnerabilidad en el Microsoft Internet Information Server. Este incidente fue un ejemplo de un raro ataque denominado "día cero", en el cual una vulnerabilidad aún sin reportar es usada para irrumpir en un sistema remoto. El servidor blanco del ataque era un servidor IIS públicamente direccionable administrado por el ejercito, aunque no era parte de la infraestructura de su sitio de red. Este servidor no guardaba información sensible ni realizaba funciones importantes.
  La vulnerabilidad aprovechada existe en un componente de Windows 2000 que es usado para manejar el protocolo de autoría y de versión de la red de cobertura mundial (WebDAV). WebDAV es un conjunto de extensiones para HTTP que permite a los usuarios editar y manejar archivos en servidores remotos. Este protocolo esta diseñado para crear aplicaciones interoperables y colaborativas que faciliten el desarrollo de software por equipos geográficamente dispersos.
  El atacante utilizó un URL especialmente formateado para generar un sobre flujo del buffer. Una vez que el sistema ha sido roto, comienza a recolectar información en la red en que se encuentra, este es un proceso conocido como "mapeo de la red". La información obtenida del mapeo de la red fue enviada de vuelta al atacante utilizando el puerto 3389, el cual es utilizado por los Servicios de Terminal Microsoft.
  No se sabe que tipo de información se obtuvo de ese servidor. Sin embargo, las direcciones de IP de otras PC en esa red e información sobre que servicios están utilizando sería muy valiosa. El personal del ejercito noto el problema después de que encontraron un incremento del análisis de la red por ese servidor. El sistema cuya seguridad fue rota también desplegaba un mensaje diciendo "Welcome to the Unicorn Beachhead", el personal del ejercito al principio reinicio el servidor, pero casi inmediatamente volvieron a irrumpir en él. Nadie sabía que era una nueva vulnerabilidad la que estaban aprovechando para el ataque. [14]

- **CASO 10**. El 25 y 26 de Marzo del 2003 los sitios en Ingles y Arábigo en Internet de la cadena de televisión Al-Jazeera sufrieron ataques sostenidos de negación de servicio

distribuido. Los ataques obligaron a la cadena a que saliera de línea por un tiempo, y forzaron a Al-Jazeera a incrementar el ancho de banda para los sitios e incrementar la seguridad en un desesperado intento por volver a estar en línea. Cada que los sitios volvían a estar en línea, rápidamente volvían a ser atacados y sacados de la red.

Los ataques comenzaron poco después de que esta cadena publicó fotos de soldados americanos hechos prisioneros en Irak. El sitio de Al-Jazeera fue golpeado por un exceso de tráfico de 200 mega bits por segundo e incluso hasta de 300 mega bits por segundo. Los sitios en Internet de esta cadena típicamente reciben un tráfico en el rango de 50 a 60 mega bits por segundo. Los ataques en contra de Al-Jazeera fueron de inundaciones al Sistema de Nombre de Dominios (DNS) en los cuales se envía un alto volumen de trafico de Internet a los servidores del nombre que son responsables por un dominio de red en particular, haciendo que no respondan esos servidores. Al-Jazeera intentó responder al ataque aumentando su ancho de banda pero no dio resultado ya que los atacantes también escalaron sus esfuerzos.

De acuerdo a expertos en seguridad, los problemas en los sitios de Al-Jazeera parecen ser causados por el ataque de un "bot" IRC y por el incremento en la demanda para entrar al sitio. Los ataques bot de IRC utilizan canales de conversación IRC para enviar instrucciones de ataques coordinados a redes de computadoras que ya han sufrido incursiones. El nivel de tráfico que golpeó Al-Jazeera puede ser generado por una red de entre 1000 y 5000 máquinas, y las redes de bots de IRC pueden contener hasta 10,000 máquinas.

Como consecuencia de este ataque, la compañía que administra los sitios de Al-Jazeera determinó que ya no podía seguir sirviendo de anfitrión a los sitios debido al efecto de los ataques en los sitios de Internet de sus otros clientes. [15]

SERVICIOS

Los servicios de seguridad son características de un programa o sistema que nos permite mantener nuestra información protegida.

- **Confidencialidad.** Nos asegura que la información en un sistema de computadora y la información transmitida sean accesibles solo por las partes autorizadas para la lectura. Este tipo de acceso incluye la impresión, desplegado, y otras formas de liberación, incluyendo la simple revelación de existencia de un objeto.
- **Autenticación.** Nos asegura que el origen de un mensaje o de un documento electrónico es correctamente identificada, y de que no se trata de una identidad falsa.
- **Integridad.** Nos asegura que solo los equipos o usuarios autorizados serán capaces de modificar las capacidades de los sistemas de computadoras y de la transmisión de información. La modificación incluye escritura, cambios, status del cambio, borrado, y retraso o revisión de los mensajes transmitidos.
- **No-repudio.** Requiere que ni la persona que envía el mensaje ni el receptor sean capaces de negar la transmisión.
- **Control de acceso.** Requiere que el acceso a las fuentes de información sea controlado por el sistema objetivo.
- **Disponibilidad.** Requiere que las capacidades del sistema de computadora estén disponibles a los equipos autorizados cuando se les necesite.

Para la aplicación de estos servicios se puede seguir las siguientes recomendaciones para la correcta elaboración de un servicio de seguridad:

1. Diseñar un algoritmo que se encargue de elaborar la transformación de seguridad.
2. Generar la información secreta que será utilizada con el algoritmo.
3. Desarrollar métodos para la distribución y la compartición de información secreta.

4. Especificar un protocolo que sea usado por los dos usuarios que haga uso del algoritmo de seguridad y la información secreta para lograr tener un servicio de seguridad.

En la figura 1.8 se observa el modelo clásico de un servicio de seguridad en red. Con las dos terminales de usuarios, el canal asegurado y el traslado de información, además del lugar típico donde se presentan los ataques. [2, capitulo 1]

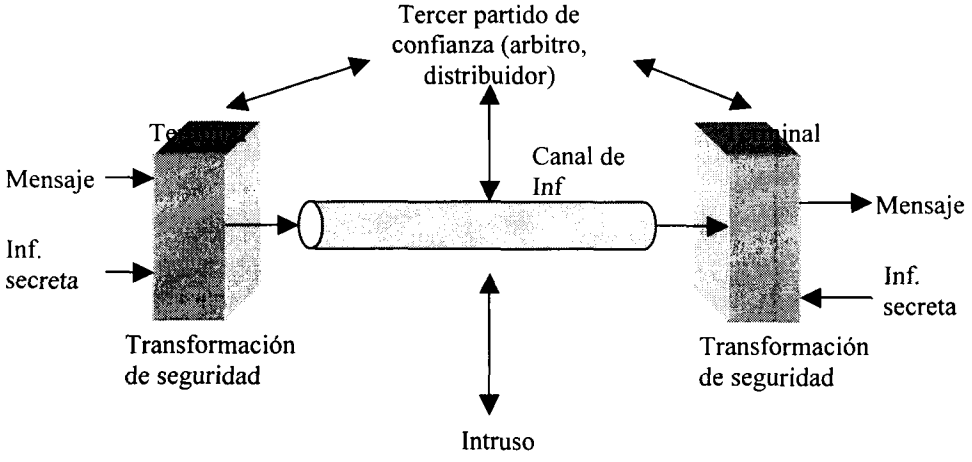


Figura 1.8 - Modelo clásico de un servicio de seguridad en red

MECANISMOS

De acuerdo a William Stallings, no hay un solo mecanismos que se encargue de proveer todos los servicios listados anteriormente. Existen varios, aunque hay una técnica constante presente en la mayoría de los mecanismos: las técnicas de criptografía. La encripción y la transformación de información son los medios más comunes para proveer seguridad. [2, capitulo 1]

NIVELES DE SEGURIDAD INFORMÁTICA

El estándar de seguridad informática más utilizado internacionalmente es TCSEC Orange Book, desarrollado en 1983 en base a las normas de seguridad de computadoras del Departamento de Defensa de los Estados Unidos. En el Orange Book se definen los niveles de seguridad para los sistemas operativos, desde un nivel mínimo hasta un nivel máximo, estos niveles también representan la base para los estándares europeos (ITSEC/ITSEM) y los internacionales (ISO/IEC). Los niveles del Orange Book son nombrados D, C1, C2, B1, B2, B3 y A.

NIVEL D.- Este nivel contiene una sola división y esta destinado para aquellos sistemas que no cumplen con ninguna especificación de seguridad. Los sistemas serían no confiables, y no habría protección para el hardware ni ningún tipo de autenticación de usuarios o de reservación de derechos de acceso a recursos. Ejemplos de sistemas que caen en esta categoría serían MS-DOS de Microsoft y System 7.0 de Macintosh.

NIVEL C1.- Este nivel se define como protección discrecional. Aquí se requiere de autenticación de los usuarios para permitir su acceso a recursos. Cada uno de los usuarios puede manejar su información privada y se hace una distinción entre los usuarios normales y los súper usuarios o

administradores del sistema. El administrador del sistema se encarga de muchas tareas de configuración y seguridad del mismo. Si en la organización se cuenta con dos o tres administradores del sistema, estos deben trabajar en forma coordinada para saber que cambios hicieron cada uno. Para que un sistema adquiera el nivel C1 debe contar con control de acceso discrecional para poder disntiguir entre usuarios y recursos, y con identificación y autenticación de usuarios antes de que comiencen a utilizar el sistema.

NIVEL C2.- Este subnivel esta dirigido a solucionar las vulnerabilidades del sistema C1, ya que cuenta con mas características de seguridad que tienen que ser cumplidas. Aquí se incluye la realización de auditorias de accesos e intentos fallidos de acceso. En este nivel se especifica la capacidad de restringir la ejecución de comandos o archivos y negar el acceso a datos de usuarios concretos, con base no solo en permisos sino también en los niveles de autorización.

La auditoria es útil ya que permite llevar registro de todas las acciones relacionadas con la seguridad, así como de las actividades realizadas por los usuarios y el administrador del sistema. La auditoria requiere de autenticación adicional, para que quien la lleve a cabo realmente sea alguien autorizado.

Los usuarios de un sistema con nivel C2 de seguridad tienen autorización para llevar a cabo operaciones de administración en el sistema sin necesidad de ser administradores.

NIVEL B1.- Este nivel se define como de protección etiquetada. Establece que el dueño del archivo no puede modificar los permisos de un objeto que esta bajo control de acceso obligado. A cada objeto del sistema (usuario, datos) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con categorías distintas (nomina, ventas, contabilidad, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa, es decir que cada usuario tiene sus objetos asociados.

NIVEL B2.- Este es el nivel de protección estructurada, esta se refiere al problema de un objeto de seguridad elevada que se comunica con un objeto de seguridad inferior. Aquí el requisito es etiquetar cada objeto de nivel superior por ser padre de un objeto inferior. El sistema es capaz de alertar a los usuarios si sus condiciones de seguridad y accesibilidad son modificadas. El administrador esta encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

NIVEL B3.- Este nivel se refiere a los dominios de seguridad. Los dominios se refuerzan con la instalación de hardware, por ejemplo el hardware de administración de memoria se encarga de proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Debe de existir un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas definidas.

Todas las estructuras de seguridad deben ser pequeñas para permitir análisis y pruebas ante posibles violaciones. En este nivel se requiere que la terminal del usuario se conecte al sistema por una conexión segura. Y no hay que olvidar que los usuarios tienen asignado los lugares y objetos a los que puede acceder.

NIVEL A.- Este es el nivel mas elevado, incluye un proceso completo de diseño, verificación, y control mediante métodos matemáticos para asegurar todos los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel, todos las recomendaciones de los niveles anteriores deben incluirse, además de que el sistema debe ser verificado en forma matemática y mediante análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados del equipo.

CAPITULO 2

MECANISMOS DE DEFENSA

Encripción

La criptografía es el arte de escribir en secreto, de transformar un texto simple a un párrafo ilegible con lo que se asegura que solo la persona que tenga la llave para leer el mensaje lo hará. Es aún la herramienta más poderosa para proporcionar seguridad computacional, al hacer que un texto sea ininteligible para el observador externo se logra que se nulifique el valor de una intercepción de los mensajes y la posibilidad de que estos sean modificados o fabricados.

Controles de Software

Los programas deben de ser lo suficientemente seguros para excluir los ataques desde afuera. También deben de ser diseñados y mantenidos para que uno pueda tener confianza en la seguridad de los programas. Los controles de software pueden incluir lo siguiente:

- Controles internos de programa
- Controles al sistema operativo
- Controles de desarrollo

Controles de Hardware

Han sido ya diseñados numerosos dispositivos que asisten en la seguridad computacional, estos van desde implementaciones de encripción en el hardware o en smartcards para asegurar el acceso limitado, protección al robo, hasta dispositivos que verifican las identidades de los usuarios.

Políticas

Son los controles más simples. Son seguidas de una administración y entrenamiento inmediatos.

Controles físicos

Algunos de los controles más fáciles y más efectivos son los físicos: cerraduras, guardias, copias de respaldo, etc.

CRIPTOGRAFÍA

La encripción nos provee de confidencialidad para los datos, adicionalmente puede ser usada para lograr tener integridad porque generalmente los datos que no pueden ser leídos no pueden ser modificados de manera significativa. Además, la encripción es la base de varios protocolos, algunos de ellos aseguran la disponibilidad de los recursos. Por tanto la encripción esta en el centro de los métodos para asegurar las tres metas de la seguridad (disponibilidad, confidencialidad e integridad). La encripción es una herramienta importante en la seguridad

computacional, pero no se le debe sobreestimar su importancia. Los usuarios deben entender que la encripción no resuelve todos los problemas de seguridad computacional. Aun más, si la encripción no se usa apropiadamente puede no tener ningún efecto en la seguridad o podría degradar el desempeño del sistema. Una encripción débil puede ser aun peor que no tener ninguna encripción, ya que da un sentimiento falso de seguridad. Por tanto es importante saber las situaciones en las cuales la encripción es útil y usarla de manera efectiva.

En un proceso de encripción, al mensaje original se le llama **texto en claro (plain text)**, y a la forma encriptada se le llama **texto cifrado (cipher text)**. En la figura 2.1 se muestra lo anterior:

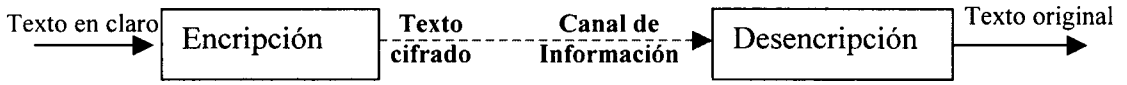


Figura 2.1- Proceso de encripción

Definamos el texto en claro como (P), el texto cifrado como (C), llaves (K), el algoritmo de encripción (E), el algoritmo de desencripción (D). Con esta nomenclatura definimos el texto cifrado como C = E(P) y el texto en claro como P = D(C). Existen en dos formas de encripción: **encripción simétrica** o encripción de una llave privada, y la **encripción asimétrica** o de llave pública.

Encripción simétrica.

En la encripción simétrica cada computadora tiene una llave secreta, que puede usar para encriptar un paquete de información antes de que este sea enviado a otra computadora por la red. La llave simétrica requiere que uno sepa que computadoras estarán comunicándose para así poder instalar la llave en cada máquina o entregarla físicamente a los usuarios de esas máquinas. La encripción por llave privada es esencialmente igual que un código secreto que deben conocer dos computadoras para decodificar la información. Este código provee la llave para decodificar el mensaje. Si alguien intercepta un mensaje codificado de esta manera no será capaz de entenderlo porque necesita la llave para traducirlo. En la encripción simétrica P = D(K, E(K, P)), debido a que D y E son procesos inversos.

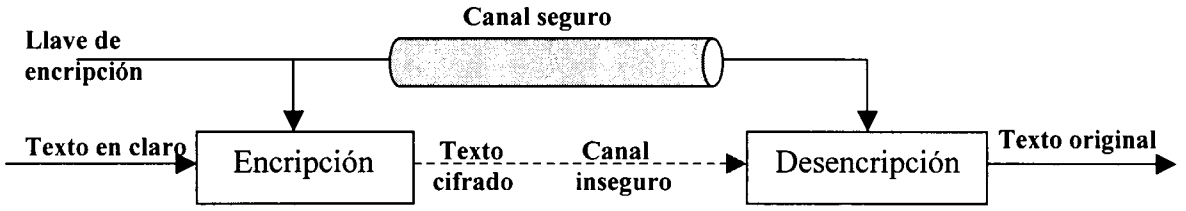


Figura 2.2 - Encripción simétrica

Son diversas las características que hacen mejor a un algoritmo de encripción simétrica para ciertas aplicaciones, a continuación presentamos algunas de estas características.

Ventajas de la encripción simétrica: [16]

- La utilización de una sola llave de encripción, permite que solo se tenga que cuidar una llave.
- Una llave de encripción de algoritmo simétrico es típicamente pequeña.
- Si se mantiene la llave segura se puede asegurar la confidencialidad y la autenticación.
- La integridad del mensaje es provista por medio del código de autenticación de mensaje (MAC) que se agrega al mensaje encriptado.
- Se tiene el estándar X9.17 de ANSI que trata acerca de la administración de llaves para facilitar el manejo de ellas.

- La encripción de mensajes largos es feasible ya que las operaciones matemáticas requieren menos tiempo que en un algoritmo de encripción asimétrica.
- Es más sencillo el envío de un texto cifrado a varios destinatarios ya que solo se maneja una sola llave privada.

Para comprender mejor la encripción simétrica veremos las desventajas generales de estos algoritmos.

Desventajas de la encripción simétrica: [16]

- La dificultad en la distribución de las llaves secretas. Para lograr la transmisión segura de una llave, si no se hace físicamente, esta debe de ser encriptada, por tanto se requiere de otra llave.
- La distribución manual de llaves es costosa, ocupa mucho tiempo y es propensa a errores.
- La necesidad de creación de centros de distribución de llaves, centros de traducción de llaves o la implementación de un algoritmo como el Diffie-Hellman para mantener el secreto de las llaves y su intercambio.

Encripción asimétrica.

La encripción asimétrica utiliza una combinación de una llave privada y una llave pública, la llave privada es conocida solo para la computadora propia, mientras que la llave pública es dada por esta computadora a cualquier computadora con la cual se quiere comunicar de manera segura. Para decodificar un mensaje encriptado, una computadora debe de usar la llave pública, provista por la computadora original y su propia llave privada. Una encripción muy popular que utiliza la utilería de llave pública es llamada Pretty Good Privacy (PGP) la cual permite encriptar casi cualquier cosa. En la encripción asimétrica el texto en claro se obtiene con $P = D(K_D, E(K_E, P))$.

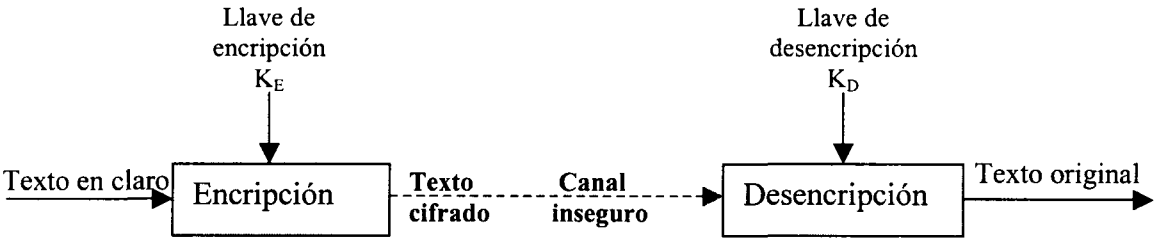


Figura 2.3 - Encripción Asimétrica

Para implementar la encripción por llave pública a gran escala, tal como un servidor de red podría necesitar, se requiere de un método diferente. Se utilizan los certificados digitales. Los certificados digitales es un bit de información que dice que el servidor es de confianza para una autoridad de certificación. La autoridad de certificación actúa como un elemento medidor en el que ambas computadoras confían. Esta confirma que cada computadora es de hecho quien dice ser, y así les provee las llaves públicas de una computadora a la otra.

La encripción asimétrica tiene sus ventajas sobre la encripción simétrica, como se ve a continuación.

Ventajas de la encripción asimétrica: [16]

- Dos usuarios pueden comunicarse sin necesidad de intercambiar llaves secretas.
- Mayor resistencia a ataques de criptoanálisis que los algoritmos de encripción simétrica.
- La encripción asimétrica provee de autenticación, integridad y servicios de no-repudio mediante la aplicación de firmas digitales.
- La distribución de llaves en un sistema de llaves públicas es más simple que en uno de llave privada, ya que las llaves públicas no hay que guardarlas en secreto.

- La encripción asimétrica requiere el uso de certificados digitales. El proceso de certificación y verificación de llaves se puede hacer en canales públicos no seguros ya que la información que se intercambia no es confidencial.

La encripción asimétrica también tiene ciertas desventajas, no siempre será la mejor opción para encriptar ciertos tipos de casos, por las siguientes razones.

Desventajas de la encripción asimétrica: [16]

- Es poco eficiente comparado con la encripción simétrica.
- Las operaciones matemáticas son más complejas y requieren más tiempo de computo.
- La encripción con algoritmos asimétricos normalmente causa que el texto cifrado resulte más grande que el texto original.
- Un mensaje encriptado por llave pública solo se puede enviar a un destinatario, ya que al usar la llave pública del destinatario para la encripción, es poco práctico enviarlo a una lista de usuarios.
- La encripción asimétrica por sí misma no provee de confidencialidad de mensaje.

La encripción asimétrica requiere mucho computo, por lo que la mayoría de los sistemas usa una combinación encripción simétrica y asimétrica. Cuando dos computadoras inician una sesión segura, una computadora crea una llave simétrica y la envía a la otra computadora usando la encripción por llave asimétrica. Las dos computadoras pueden entonces comunicarse utilizando encripción por llave simétrica. Una vez que la sesión es finalizada, cada computadora descarta la llave simétrica usada para esa sesión. Cualquier sesión adicional requiere que una nueva llave simétrica sea creada y el proceso se repite. La llave en la encripción por llave asimétrica se basa en el valor *hash*.

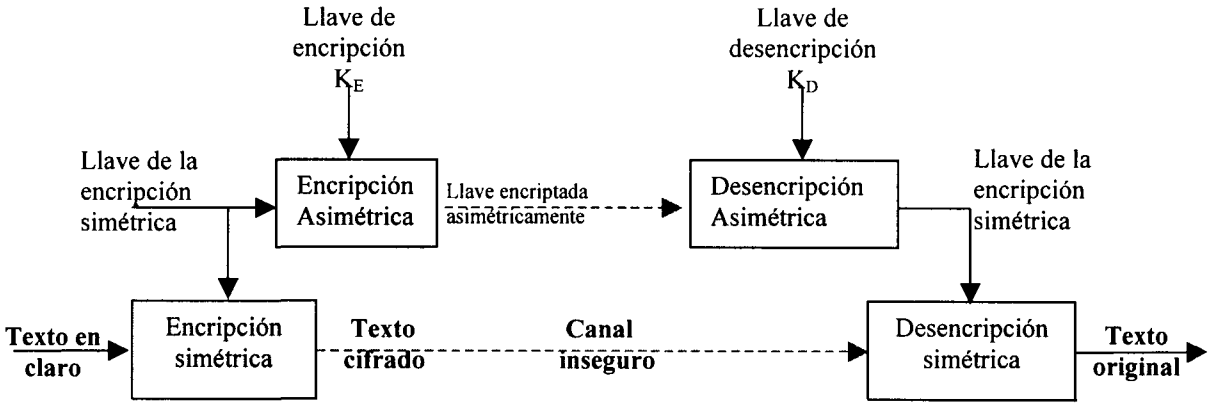


Figura 2.4 - Utilización conjunta de la encripción simétrica y asimétrica

En la figura 2.4 podemos ver de forma grafica la utilización conjunta del sistema simétrico y asimétrico de encripción, en donde un mensaje se encripta simétricamente y la llave de esta encripción también es codificada de manera asimétrica para su transmisión segura. Antes de presentar algunos algoritmos de encripción simétrica y asimétrica, se muestra en la tabla 2.1 un resumen de las principales características de la encripción simétrica y asimétrica y poder apreciar sus diferencias y similitudes.

Tabla 2.1- Características principales de los algoritmos de encripción simétrica y asimétrica

Algoritmos Encripción Simétrica	Algoritmos de Encripción Asimétrica
Utilización de una sola llave para la encripción y desencripción.	Utilización de dos llaves, una llave pública para encriptar y una llave privada para desencriptar.
La encripción simétrica provee de confidencialidad y autenticación del mensaje.	La encripción asimétrica provee de autenticación, integridad y servicios de no-repudio mediante las firmas digitales.
Para garantizar la integridad del mensaje se hace uso del código de autenticación de mensaje (MAC).	Requiere el uso de certificados digitales y autoridades certificadoras para asegurar la identidad del origen y destinatario en un sistema de encripción asimétrica.
La llave de encripción típicamente es más pequeña que la de encripción asimétrica.	Normalmente el texto encriptado de manera asimétrica es más grande que el texto original.
La encripción simétrica presenta una buena resistencia a los ataques de criptoanálisis, aunque no tan alta como la encripción asimétrica.	La encripción asimétrica presenta una mayor resistencia al criptoanálisis.
Como se maneja una sola llave secreta, es posible enviar el mensaje a una lista de usuarios.	Con el sistema de llave pública un mensaje solo puede enviarse a un usuario, porque se utiliza la llave pública exclusiva de este usuario.
Es posible la encripción de mensajes largos ya que las operaciones matemáticas requieren poco tiempo de procesamiento.	La eficiencia es menor ya que requiere de más tiempo de procesamiento para realizar las operaciones matemáticas de encripción.
Si las llaves secretas no se distribuyen físicamente, se necesita un canal seguro para distribuirlas, o que sean encriptadas de forma asimétrica.	Pueden hacer uso de canales públicos no seguros para el proceso de certificación, ya que la información transferida es de conocimiento público.
Requiere de centros de distribución y centros de traducción de llaves.	No es necesario tener centros de distribución de llaves, ya que las de encripción son públicas.

ALGORITMOS DE CRIPTOGRAFÍA SIMÉTRICA

DES (Data Encryption Standard):

Es el esquema de encripción más ampliamente usado, fue adoptado en 1977 por el National Bureau Standards, ahora National Institute of Standards and Technology. En el algoritmo DES, los datos son encriptados en bloques de 64 bits utilizando una llave de 56 bits. El algoritmo transforma la entrada de 64 bits a través de una serie de pasos en una salida de 64 bits, y los mismos pasos, con la misma llave son usados para revertir la encripción.

La encripción sucede de la manera que sigue. Primero al texto de 64 bits se le aplica una permutación inicial que reacomoda los bits. Esto es seguido de una fase de 16 ciclos de la misma función, lo cual envuelve funciones de permutación y sustitución. La salida del último ciclo consiste de 64 bits que son función de la entrada en claro y de la llave. Esta salida se divide a la mitad en bloques de 32 bits, las partes izquierda y derecha de la salida son intercambiadas para producir una pre-salida. Finalmente esta pre-salida es pasada a través de una permutación inversa a la primera que se aplicó, para producir un texto cifrado de 64 bits.

La llave no se usa directamente como es, sino que pasa a través de una función de permutación. Y para cada uno de los 16 ciclos se produce una sub-llave K_i combinando un cambio circular hacia la izquierda y una permutación.

El tener una llave de 56 bits nos permite tener 2^{56} posibles llaves, lo cual es aproximadamente 7.2×10^{16} llaves. Si se tuviera una máquina con una velocidad de procesar una encripción DES por microsegundo le tomaría más de mil años romper el cifrador, aunque con los avances en la rapidez de las computadoras estos tiempos se han reducido enormemente, hasta el punto en que se pueden lograr encontrar 50 millones de llaves por segundo con un equipo dedicado.

IDEA (International Data Encryption Algorithm) :

El Algoritmo Internacional de Encripción de Datos (IDEA), es un algoritmo simétrico de cifrado de bloque diseñado por Xuejia Lai y James Massey del Instituto de Tecnología Federal Suizo. Fue propuesto para reemplazar a DES.

IDEA usa una llave de 128 bits para encriptar los datos que son divididos en bloques de 64 bits. Como en cualquier esquema de encripción hay dos entradas para la función de encripción: el texto inicial a ser encriptado y la llave.

El bloque de datos de 64-bits se divide en cuatro sub-bloques de 16 bits: X_1, X_2, X_3 y X_4. Estos cuatro sub-bloques son la entrada del primer ciclo del algoritmo. Tiene ocho ciclos en total. En cada vuelta a los cuatro sub-bloques se les aplica XOR y son sumados y multiplicados bit a bit con seis sub-bloques de 16 bits de sub-llaves. Entre ciclos, el segundo y tercer sub-bloque se intercambian. Finalmente, los cuatro sub-bloques se combinan con cuatro sub-llaves en una transformación de salida.

En cada ciclo, la secuencia de eventos se da como sigue:

[1] Multiplicación de X_1 y la primera sub-llave.
[2] Suma de X_2 y la segunda sub-llave.
[3] Suma de X_3 y la tercer sub-llave.
[4] Multiplicación de X_4 y la cuarta sub-llave.
[5] XOR del resultado de los pasos [1] y [3].
[6] XOR del resultado de los pasos [2] y [4].
[7] Multiplicación de los resultados del paso [5] con la quinta sub-llave.
[8] Suma de los resultados de los pasos [6] y [7].
[9] Multiplicación de los resultados del paso [8] con la sexta sub-llave.
[10] Suma los resultados del paso [7] y [9].
[11] XOR del resultado de los pasos [1] y [9].
[12] XOR del resultado de los pasos [3] y [9].
[13] XOR del resultado de los pasos [2] y [10].
[14] XOR del resultado de los pasos [4] y [10].

La salida del ciclo es de cuatro sub-bloques que tienen el resultado de los pasos [11], [12], [13] y [14]. Se intercambian los dos bloques internos (excepto para el último ciclo) y esto es la entrada del próximo ciclo.

Después de ocho ciclos, existe una transformación de salida final:

[1] Multiplicación de X_1 y la primera sub-llave.
[2] Suma de X_2 y la segunda sub-llave.
[3] Suma de X_3 y la tercer sub-llave.
[4] Multiplicación de X_4 y la cuarta sub-llave.

Finalmente, los cuatro sub-bloques son readjuntados para producir el texto cifrado.

El proceso de desencripción es básicamente el mismo que el de encripción. Se usa el texto cifrado a manera de entrada para la misma estructura de IDEA solo que con diferentes llaves. Las llaves de desencripción son obtenidas a partir de las llaves de encripción.

El algoritmo IDEA supone la utilización de 52 sub-llaves de 16 bits las cuales son generadas a partir de la llave de encripción de 128 bits. El proceso es como se describe enseguida:

- Las primeras ocho sub-llaves, las cuales podemos identificar como Z_1, Z_2, ...,Z_8, son tomadas directamente de la llave principal, con Z_1 siendo igual a los primeros 16 bits más significativos de la llave, Z_2 corresponde a los siguientes 16 bits y así sucesivamente.
- Después de esto se hace un cambio circular hacia la izquierda de 25 posiciones de bits en la llave de encripción, y con esto se extraen las siguientes ocho sub-llaves.
- Este procedimiento se repite hasta que las 52 sub-llaves son generadas.

Esto nos da un esquema bastante seguro de variación de sub-llaves para usarlos en los ocho ciclos. Cada sub-llave utiliza un diferente conjunto de bits de la llave de encripción.

TRIPLE DES :

Este algoritmo se originó para evitar los ataques del tipo "*man-in-the-middle* " por que hace uso de tres estaciones de encripción con tres diferentes llaves. Por lo que aumenta el requerimiento de texto en claro conocido hasta 2^{112} lo cual esta mas allá de lo práctico. Sin embargo, también requiere una llave muy larga de 56 x 3 = 168 bits.

Hay ataques para el TRIPLE DES que utiliza dos llaves; para esto se diseño el TRIPLE DES que maneja 3 llaves, este tiene una llave efectiva de 168 bits y es definida en la ecuación 1 como sigue:

$$C = E_{K3}\,[D_{K2}[E_{K1}[P]]] \qquad (1)$$

Un buen número de aplicaciones de Internet han adoptado este algoritmo, incluyendo PGP y S/MIME.

BLOWFISH :

Blowfish es un cifrador de bloques simétrico desarrollado por Bruce Schneier, y tiene las siguientes características:

- **Rápido**: Blowfish encripta datos en microprocesadores de 32 bits a una razón de 18 ciclos por byte.
- **Compacto**: Blowfish puede correr en menos de 5K de memoria.
- **Simple**: Blowfish tiene una estructura simple la cual es fácil de implementar y facilita la tarea de determinar la fuerza del algoritmo.
- **Seguridad Variable**: La longitud de la llave es variable y puede ser hasta de 448 bits. Esto permite que se pueda definir si se requiere alta velocidad o alta seguridad.

Blowfish hace uso de una llave que va de 32 a 448 bits. Esta llave es usada para generar 18 sub-llaves de 32 bits y cuatro 8x32 S-boxes conteniendo un total de 1024 entradas de 32 bits.

Las llaves son grabadas en un arreglo K, las sub-llaves son grabadas en un arreglo P, hay 4 S-boxes, cada una de 256 entradas de 32 bits. Un total de 521 ejecuciones del algoritmo de encripción son requeridas para producir los arreglos finales S y P. Por tanto, Blowfish no es apropiado para aplicaciones en las cuales las llaves cambien frecuentemente. Para ejecuciones rápidas, los arreglos P y S pueden ser almacenados en lugar de ser derivados de la llave cada vez que el algoritmo es utilizado. Esto requiere de 4K de memoria por lo que Blowfish no es apropiado para aplicaciones con memoria limitada, tales como las smartcards.

RC5 :

Desarrollado por Ron Rivest. RC5 fue diseñado para tener las siguientes características:

- **Apropiado para hardware o software**: RC5 utiliza solo operaciones computacionales primarias comúnmente encontradas en los microprocesadores.
- **Rápido**: RC5 es un algoritmo simple y esta orientado a palabras. Las operaciones básicas trabajan con palabras completas de datos.
- **Adaptables a procesadores de diferentes tamaños de palabras**: El número de bits en una palabra es un parámetro de RC5. Diferentes tamaños de palabras nos dan diferentes algoritmos.
- **Número variable de ciclos**: El número de ciclos es un segundo parámetro de RC5. Este parámetro permite un intercambio entre mayor seguridad o mayor velocidad.
- **Longitud variable de llave.**
- **Simple**: RC5 tiene una estructura que es fácil de implementar y facilita la tarea de determinar la fortaleza del algoritmo.
- **Bajo requerimiento de memoria**: Un bajo requerimiento hace a RC5 apropiado para smartcards.
- **Alta seguridad**: RC5 es diseñado para proveer alta seguridad con parámetros apropiados.
- **Rotaciones dependientes de los datos**: RC5 incorpora rotaciones (cambios circulares de bit) cuyo monto depende de los datos. Esto refuerza el algoritmo contra el criptoanálisis.

RC5 utiliza operaciones primarias y sus inversos:

- **Adición:** Adición de palabras, denotadas por +, es desempeñada 2^w. El inverso, denotado por "–" es la substracción 2^w.
- **OR exclusivo de Bit**: Esta operación es denotada por ⊕.
- **Rotación circular a la izquierda.**

RC5 es realmente una familia de algoritmos de encripción determinados por tres parámetros como se muestra en la tabla 2.2:

Tabla 2.2 - Algoritmos de encripción

Parámetro	Definición	Valores permitidos
w	Tamaño de palabra en bits. RC5 encripta bloques de 2 palabras	16, 32, 64
r	Número de ciclos	0,1...,255
b	Número de 8 bytes (octetos) en la clave secreta K	0,1...,255

Por tanto RC5 encripta bloques de texto en claro de longitudes de 32, 64 o 128 bits en bloques de texto cifrado de la misma longitud. La longitud de la llave va desde 0 a 2040 bits. Una

versión especifica de RC5 es designada como RC5-w/r/b. Por ejemplo, RC5-32/12/16 tiene palabras de 32 bits, 12 ciclos de encripción y desencripción, y una longitud de llave de 16 bytes (128 bits).

CAST-128 (Carlisle Adams & Stafford Tavares) :

CAST fue diseñado para los algoritmos de encripción simétrica por Carlisle Adams & Stafford Tavares. CAST utiliza una llave que varia desde 40 bits hasta 128 bits en incrementos de 8 bits. CAST tiene la estructura de una red Feistel con 16 ciclos y operando con bloques de 64 bits de texto en claro para producir bloques de 64 bits de texto cifrado, además de que incluye dos sub-llaves en cada ciclo: una de 32 bits K_{mi} y otra de 5 bits K_{ri}. Y la función F depende del ciclo.

CAST es el resultado de un largo proceso de investigación y desarrollo y se esta comenzando a implementar en PGP. CAST-128 utiliza cuatro operaciones primarias: **Adición, substracción, OR exclusivo, rotación circular izquierda**. La encripción comienza cuando el texto en claro es dividido en dos partes de 32 bits L_0 y R_0. El texto cifrado es formado intercambiando las salidas del ciclo dieciséis, es decir, la concatenación de R_{16} y L_{16}.

CAST-128 utiliza 8 x 32 S-boxes (Cajas de sustitución) cuatro de estas son usadas en la encripción y desencripción. Las cuatro restantes, son utilizadas en la generación de sub-llaves. Cada S-box es un arreglo de 32 columnas y 256 filas. La entrada de 8 bits selecciona una fila en el arreglo; el valor de 32 bits en esa fila es la salida. Todas las S-boxes contienen valores fijos.

ALGORITMOS DE CRIPTOGRAFÍA ASIMÉTRICA

RSA (Rivest-Shamir-Adleman):

Desarrollado en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT. Es el único algoritmo que ha reinado en el campo de la criptografía de llave pública. El esquema de RSA es un cifrador de bloque en donde el texto en claro y el texto cifrado son enteros entre 0 y n-1 para algunas n.

El texto en claro es encriptado en bloques, con cada bloque teniendo un valor binario menor que algún número n. El tamaño del bloque debe de ser menor o igual a $\log_2(n)$; en la práctica el tamaño del bloque es 2^k bits. La encripción y desencripción son como se ve en las ecuaciones (2) y (3), para un bloque de texto en claro M y un bloque de texto cifrado C.

$$C=M^e \bmod n \qquad (2)$$
$$M=C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n \qquad (3)$$

El que envía y el que recibe deben conocer el valor de n. Quien envía sabe el valor de *e*, y solamente el receptor sabe el valor de *d*. Por tanto este es un algoritmo de llave pública con una llave de KU={e,n} y una llave privada de KR={d,n}. Para que este algoritmo sea satisfactorio para la encripción de llave pública, los siguientes requerimientos deben ser logrados:

1.- Es posible encontrar valores de *e, d, n*, tales que $M^{ed}=M \bmod n$ para todo $M<n$
2.- Es relativamente fácil calcular M^e y C^d para todos valores de $M<n$.
3.- Es infeasible determinar *d* dado *e* y *n*.

Para resumir el algoritmo RSA veamos la tabla 2.3:

Tabla 2.3 - Algoritmo RSA

Generación de llaves

Seleccionar p,q	P y q son primos
Calcula n =p x q	
Calcula $\phi(n)=(p-1)(q-1)$	
Selecciona el entero e	$Gcd(\phi(n),e)=1;1<e<\phi(n)$
Calcula d	$D=e^{-1} \bmod \phi(n)$
Llave pública	KU={e,n}
Llave privada	KR={d,n}

Encripción

Texto claro	M<n
Texto cifrado	$C=M^e \pmod n$

Desencripción

Texto claro	C
Texto cifrado	$M=C^d \pmod n$

Diffie-Hellman:

Este fue el primer algoritmo publicado que apareció en el artículo de seminario de Diffie y Hellman el cual definió la criptografía de llave pública y normalmente se le llama intercambio de llaves de Diffie-Hellman. Un buen número de productos comerciales emplea esta técnica de intercambio.

El propósito de este algoritmo es permitir a dos usuarios intercambiar una llave de manera segura para que después pueda ser usada para la encripción de mensajes. El algoritmo por sí mismo esta limitado al intercambio de llaves. Este algoritmo depende para su efectividad de la dificultad de calcular algoritmos discretos.

Tabla 2.4 - Algoritmo Diffie-Hellman

Elementos públicos globales

Q	Número primo
α	$\alpha<q$ y α una raíz primaria de q

Generación de llave del usuario A

Seleccionar X_A privada	$X_A<q$
Calcular Y_A pública	$Y_A = \alpha^x A \bmod q$

Generación de llave del usuario B

Seleccionar X_B privado	$X_B<q$
Calcular Y_B publico	$Y_B=\alpha^x B \bmod q$

Generación de la llave secreta por el usuario A

$K=(Y_B)^x A \bmod q$

Generación de la llave secreta del usuario B

$K=(Y_A)^x B \bmod q$

FUNCIONES HASH

Una función *hash* es una función de transformación sin-llave, dado un mensaje de tamaño variable como entrada, la función *hash* produce una representación de tamaño fijo como salida. Quizás la principal utilidad de las funciones *hash* es que sirven para verificar la integridad de un mensaje y para aplicar las firmas digitales. Los cálculos de las funciones *hash* son generalmente más rápidos que los algoritmos de encripción o de firma digital, por ello muchas veces se aplica un procesamiento criptográfico al valor *hash* del documento, el cual es más pequeño que el documento mismo.

Un valor *hash* es generado por una función H de la forma:

$$h=H(M) \tag{4}$$

Donde M es un mensaje de longitud variable y H(M) es el *valor hash* de longitud fija. El *valor hash* es añadido al mensaje en la fuente en un momento en que se sabe que el mensaje es correcto. El receptor verifica el mensaje volviendo a obtener el *valor hash*. Como las funciones hash no son secretas existen algunos métodos para proteger el *valor hash*. Los cuales consisten en el envío a través de un canal seguro o de diversas maneras que incluyen la encripción.

Si se utiliza un valor *hash* es prácticamente imposible encontrar en valor original sin saber los datos que se usaron para crear el valor *hash*. Un ejemplo simple:

Número de entrada	Algoritmo Hash	Valor Hash
10,667	Input # x 143	1,525,381

Para que una función *hash* sea utilizada en la autenticación es necesario que cumpla ciertos requerimientos. El propósito de estas funciones es proporcionar una "huella digital" de un archivo, mensaje o bloque de datos. Para que sea útil la función debe de cumplir la lista que tenemos a continuación:

1. La función H debe de poder ser aplicada a un bloque de datos de cualquier tamaño.
2. H produce una salida de longitud fija.
3. H(x) es relativamente fácil de calcular para cualquier x dada, haciendo la implementación de hardware y software práctica.
4. Para cualquier código h dado, es computacionalmente improbable encontrar x tal que H(x)=h. A esto se le llama en la literatura función de **un-sentido.**
5. Para cualquier bloque x dado, es computacionalmente improbable encontrar $y \neq x$ con H(y) = H(x). A esto generalmente se le llama **débil resistencia a las colisiones**.
6. Es computacionalmente improbable encontrar cualquier par (x,y) tal que H(x)=H(y). A esto a veces se le llama **resistencia fuerte a las colisiones.**[2, capitulo 8]

De la cuarta propiedad podemos deducir que es fácil generar un código dado un mensaje, sin embargo es prácticamente imposible generar un mensaje dado un código. Esto es importante si la técnica de autenticación involucra el uso de un valor secreto. Este valor secreto que se puede interpretar también como el *valor hash*. El valor secreto no es enviado, aunque si la función *hash* no es de un solo sentido un atacante puede descubrir el valor secreto. Si un atacante observa la comunicación, el atacante puede obtener el mensaje M y el código *hash* $C=H(S_{AB}||M)$, el atacante puede invertir la función *hash* para obtener $S_{AB}||M = H^{-1}(c)$. Como el atacante ahora tiene M y $S_{AB}||M$ es fácil obtener S_{AB}.

La quinta propiedad garantiza que un mensaje alternativo que este relacionado con el mismo valor *hash* no puede ser encontrado, de lo contrario el atacante podría leer el mensaje y

generar su propio código *hash*. Pero como el oponente no tiene la llave secreta no puede alterar el mensaje sin que sea detectado. Una secuencia típica para un atacante, si lo anterior fuera falso, sería interceptar el mensaje junto con su código *hash* encriptado; segundo, generar un código *hash* no encriptado a partir del mensaje M; tercero, generar un mensaje alternado con el mismo código *hash*.

La sexta propiedad se refiere a cuan resistente es la función *hash* contra ciertos tipos de ataques.

Todas las funciones *hash* se manejan bajo los mismos principios básicos. La entrada es vista como la secuencia de bloques de n-bits. La entrada es procesada un bloque a la vez de una manera iterativa para producir una función *hash* de n-bits. Una de las funciones *hash* más sencillas es la de *bit-por-bit* OR exclusivo (XOR) de cada bloque, esto puede expresarse como sigue:

$$C_1 = b_{i1} \oplus b_{i2} \oplus \ldots \oplus b_{im} \qquad (5)$$

Donde C_i = i-ésimo bit del código hash, $1 \leq i \leq n$
m = número de bloques de n-bits en la entrada
b_{ij} = i-ésimo bit en el bloque j-ésimo
$\oplus$ = Operación XOR

Esta operación produce una paridad simple para cada posición de bit y es conocido como un chequeo de redundancia longitudinal. Es razonablemente efectivo para datos aleatorios como un chequeo de integridad de datos. Cada valor *hash* de n-bit es igualmente probable. Por tanto, la probabilidad de que un error de datos resulte en un valor hash no cambiado es 2^{-n}. En la mayoría de los archivos de texto normal, el bit de alto orden de cada octeto es cero. Así que, si se usa un valor *hash* de 128 bits, en lugar de tener una efectividad de 2^{-128}, la función *hash* en este tipo de datos tiene una efectividad de 2^{-112}. Una manera de mejorar el algoritmo es ejecutar un cambio circular, o rotación del valor *hash* después de que cada bloque es procesado. El proceso puede resumirse como sigue:

1.- Inicialmente colocar en cero el valor *hash* de n-bits.
2.- Procesar cada bloque de datos sucesivo de n-bits como sigue:
- Rotar el valor *hash* actual a la izquierda un bit
- XOR el bloque dentro del valor *hash*.

Esto tiene el efecto de hacer la entrada más completamente aleatoria y sobrepasar cualquier regularidad que aparece en la entrada. Aunque el segundo procedimiento provee de una buena medida de la integridad de los datos, es virtualmente inútil para la seguridad de los datos cuando un código *hash* encriptado es utilizado con un mensaje de texto simple. Dado un mensaje, es fácil producir un nuevo mensaje que nos dé el código *hash*, simplemente se prepara el mensaje alterno deseado y entonces adjunta un bloque de n-bits que forcé el nuevo mensaje más el bloque para encontrar el código *hash* deseado. **[2, capitulo 8]**

Las llaves públicas generalmente usan algoritmos complejos y valores *hash* muy largos para la encripción, incluyendo números de hasta 40-bits o 128 bits. Como sabemos un número de 128 bits tiene 2^{128} combinaciones. Entre las funciones *hash* más conocidas y utilizadas están: **MD2**, **MD4**, **MD5** y **SHA**.

CAPITULO 3

PROTOCOLOS DE SEGURIDAD

EL PROTOCOLO DE INTERNET 6

Internet opera hoy en día por medio del IPv4. Un protocolo de Internet se le considera como un protocolo internetwork esto es porque puede operar con los diferentes protocolos de otras subcapas tales como el de Ethernet, el modo de transferencia asíncrono (ATM) y servicios integrados de redes digitales (ISDN)[17]. El protocolo provee un formato de paquete estándar que los demás subprotocolos son capaces de transportar. Uno puede decir que el protocolo internetwork esta definido por su formato básico de paquete y por el tipo de servicios que provee. El IPv4 ya tiene varios años funcionando y debido a las actuales demandas en desempeño en los nodos de ruteo así como el rápido consumo de las direcciones y el hecho que el IPv4 no tiene características incluidas de seguridad sino que más bien se ha tenido que auxiliar del IPsec para proporcionar un cierto nivel de seguridad, son las muestras de que este protocolo esta llegando al final de su vida útil. [18]

El Protocolo de Internet en su versión 4 (IPv4) fue creado cuando se pensaba que su número máximo de direcciones posibles que es de alrededor de 4 mil millones de direcciones (2^{32}); pero al ritmo que ha avanzado la tecnología y dadas las facilidades para tener una computadora conectada a la red esta cifra se alcanzara en esta misma década, aunado a esto se pensó también que el sucesor del IPv4 debería tener capacidades para poder asegurar la transferencia de paquetes para evitar los principales ataques que se gestan en la red. A manera de solucionar todas estas dificultades que se han presentado con el paso de los años se diseño un nuevo protocolo, el IPv6. [19]

En 1991 la IETF (Internet Engineering Task Force) sintió la necesidad de crear una mesa directiva que se encargara del desarrollo del protocolo de Internet para la siguiente generación. Para esto fue nombrado un Directorado para el protocolo de siguiente generación (IPng). En Junio de 1992 el Directorado recibió tres propuestas, las cuales fueron:

- TCP y UDP con direcciones más grandes (TUBA).
- IP versión 7.
- Simple IP Plus.

El Directorado de IPng analizó todas estas propuestas en Junio de 1994. Y entonces sugirió al Simple IP Plus (SIPP) como la base para el nuevo IP, pero cambiándole algunas de sus características. Pasó casi un año para que se finalizaran de definir las especificaciones del IPv6.

Los cambios del IPv4 al IPv6 en cuanto a las características del encabezado (*header*) de los paquetes de información fueron principalmente en la simplificación de algunos de los campos y de cambios en sus tamaños. A continuación se mencionan algunas de las ventajas con las que cuenta el IPv6 sobre el IPv4:

- **Una mayor cantidad de direcciones IP.** El esquema de direccionamiento del IPv4 puede soportar un máximo teórico de 4.29 mil millones de direcciones IP. Sin embargo, debido a las ineficiencias de operación, tales como la necesidad de tener suficientes direcciones para las configuraciones de subnet dentro de Internet han limitado las direcciones útiles de IP a solo 200 millones. Esta cantidad de direcciones no será suficiente para soportar la increíble demanda de la industria, ya que en unos cuantos años habrá celulares, dispositivos portátiles, sistemas embebidos y juegos de video que se conectaran a Internet, con lo que aumentara él trafico en los nodos de ruteo. Uno de los métodos que se usan para lidiar con este desabasto de direcciones es el usado por varias organizaciones, la tecnología de traducción network-address (NAT). NAT permite a las compañías crear grandes números de direcciones de Internet privadas y sin registrar para uso interno. Estas direcciones privadas se conectan a Internet vía un limitado número de direcciones públicas registradas, sin embargo este método crea vulnerabilidades y otros problemas. El IPv6 ofrece un esquema de direccionamiento de 128 bits.
- **Extensibilidad y seguridad**. El IPv4 aporta la extensibilidad, sin embargo se limita a solo 40 bytes el monto de los datos que pueden usarse para describir la funcionalidad adicional provista por las extensiones. El IPv6 permite opciones más grandes de descripción para que así las extensiones puedan agregar funcionalidad tales como una seguridad mejorada y control de ruteo. El IPv6 provee de autenticación, confidencialidad e integridad de los paquetes en la red. Para lograr esto el IPv6 incluye dos nuevas características el Authentication Header (AH) y el Encapsulated Security Payload (ESP). El AH nos da los mecanismos para la autenticación e integridad para detectar si un paquete ha sido modificado durante la transmisión. El ESP garantiza que solo los receptores legítimos sean capaces de acceder a la información.
- **Autoconfiguración**: El enorme número de direcciones de IPv6 permitirá que cada dispositivo en la red tenga su propia dirección. Esto eliminará la necesidad de una configuración manual. [20]

La política actual para la localización de dirección con el IPv6 es la de agregar un prefijo de 48 bits a cada sitio en Internet ya sean hogares, empresas o pequeñas oficinas. El prefijo de 48 bits permite que haya 65,000 subredes dentro de cada sitio, cada una de ellas podrá acomodar un número prácticamente infinito de hosts. Desde 1996 se han estado haciendo pruebas con este protocolo a través de una red de investigación y de sites comerciales a la que se le llamó 6Bone. [20][21]

Sin embargo, hasta hace muy poco tiempo, los vendedores de Sistemas Operativos han comenzado a agregar en su software soporte para este protocolo, además de que los administradores de redes y los proveedores de Internet están haciendo este cambio de una manera muy lenta, esto hasta cierto punto es normal y entendible ya que los administradores de redes no pueden dar por hecho que este nuevo protocolo sea soportado por todo el software que ya existe. No todos se pueden confiar en las promesas de que este es el protocolo que se usara, sin embargo hay mucha gente que ya se esta animando a agregar el soporte necesario para que ahora muchos de los servidores sean capaces del transporte de información bajo el IPv6.

En 1997 IBM fue el primer abastecedor de software y equipo con UNÍS el cual ofrecía su sistema operativo con una pila TCP/IP que soportaba IPv6, en este caso fue para el servidor RS/6000, además de que también se incluyó el soporte para servidores OS/390 y OS/400 con LINUX.

Cisco Systems ha diseñado ruteadores IOS (Internetworks Operating Systems) los cuales también incluyen el soporte para IPv6, este es un hecho muy importante ya que los ruteadores de Cisco portan el 80% del trafico principal de Internet. La compañía Microsoft también ha incluido un previo de tecnología de desarrollador IPv6 en el Service Pack para Windows 2000 y el soporte del IPv6 de igual manera esta presente en la versión del Explorador de Internet para Windows XP. El hecho de que Microsoft incluya este soporte es otro paso muy importante en el camino de la

implementación total del IPv6 ya que esto permite que otras compañías desarrollen aplicaciones para los millones de usuarios de Windows tales como la telefonía por Internet.

Sun Microsystems construyó el apoyo para el IPv6 dentro de su sistema Solaris 8 OS al igual que en la última versión del Java Development Kit.

Varias compañías japonesas también se dedican a incluir en sus productos el soporte para el IPv6, por ejemplo: el ruteador GeoStream R940 de Fujitsu, el ruteador backbone GR2000 de Hitachi, el ruteador y portal de seguridad IPv6 de Matsushita (Panasonic), y el conmutador de NEC de las series IP8800/700. Además de que la compañía Sony esta trabajando con Cisco para desarrollar una pila (*stack*) dual IPv4/IPv6 para el acceso a Internet de su consola para juegos de video Playstation2.[22][23]

CAMBIOS EN EL ENCABEZADO DE LA VERSIÓN IPv4 A LA IPv6

El encabezado del IPv6 esta basado en el del IPv4 al cual se le agregaron campos y se le quitaron algunos que casi no se usaban o eran redundantes. Un encabezado del IPv4 tiene los siguientes campos y sus siguientes dimensiones:

- Versión.....4 bits.
- Longitud del Header .....8 bits
- Tipo de servicio.....8 bits
- Longitud total.....15 bits
- Identificación de fragmentos.....15 bits
- Banderas.....2 bits
- Desplazamiento de fragmentos.....13bits
- Limite de salto.....8 bits
- Protocolo.....8 bits
- Check sum.....15 bits
- Dirección de la fuente.....32 bits
- Dirección del destino.....32 bits
- Opciones.....24 bits
- Padding .....7 bits

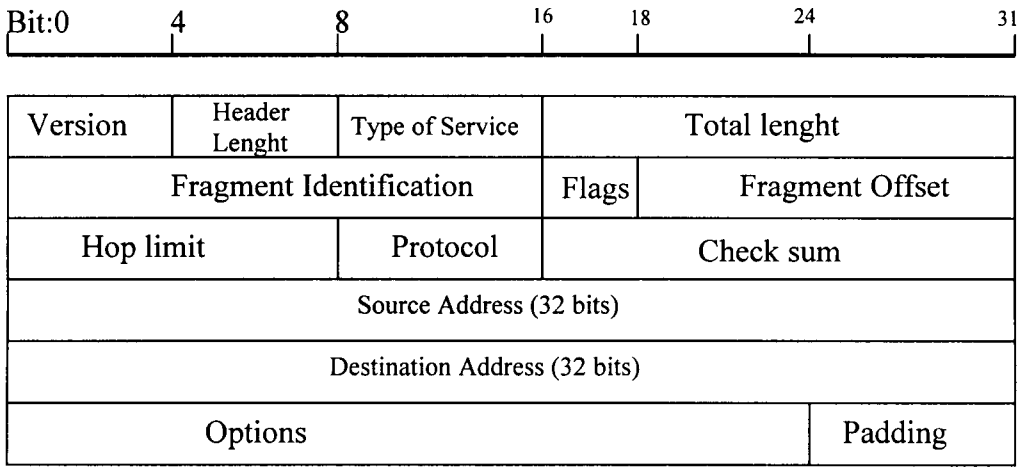


Figura 3.1 - Formato del encabezado del IPv4

El encabezado del IPv6 tiene un formato de longitud fija por lo que el campo de longitud de encabezado ya es inútil y fue descartado. También fue removido el campo de *checksum* ya que los procedimientos de MAC del estándar 802 de la IEEE y capas de la AAL de la ATM al igual que los procedimientos de punto-a-punto ya tienen *checksum*. El campo de tipo de servicio, el cual era muy raramente utilizado también fue removido. El procedimiento de segmentación de salto-por-salto fue quitado y el campo de procedimiento ha sido cambiado por el campo de prioridad.

El procedimiento de descubrir la trayectoria MTU (Maximum Transmission Unit) le dice a la aplicación el tamaño máximo aceptado del segmento de manera que paquetes mayores son rechazados. La fragmentación no es necesitada mas dentro de la red. IPv6 no fragmenta paquetes de mayor tamaño del permitido. Si un paquete es mayor que el mayor MTU permitido del siguiente salto, el paquete será rechazado y un mensaje de ICMP será enviado de regreso. Aun así existe la posibilidad de utilizar uno de los encabezados opcionales para permitir la fragmentación de un paquete con longitud mayor que la permitida por el MTU.

En este aspecto IPv6 requiere que el MTU de cada eslabón en Internet sea de 576 octetos o mayor. El procedimiento de descubrir la trayectoria MTU es muy útil ya que si se aplica es posible que los nodos de IPv6 saquen mejor provecho de trayectorias con un MTU mayor a 576 octetos

El encabezado (*header*) del IPv6 y sus campos son los siguientes:

- Versión.....4 bits
- Prioridad.....4 bits
- Etiqueta de flujo.....23 bits
- Longitud de Payload.....16 bits
- Siguiente *header*.....8 bits
- Limite de salto.....7 bits
- Dirección de fuente.....128 bits
- Dirección de destino.....128 bits

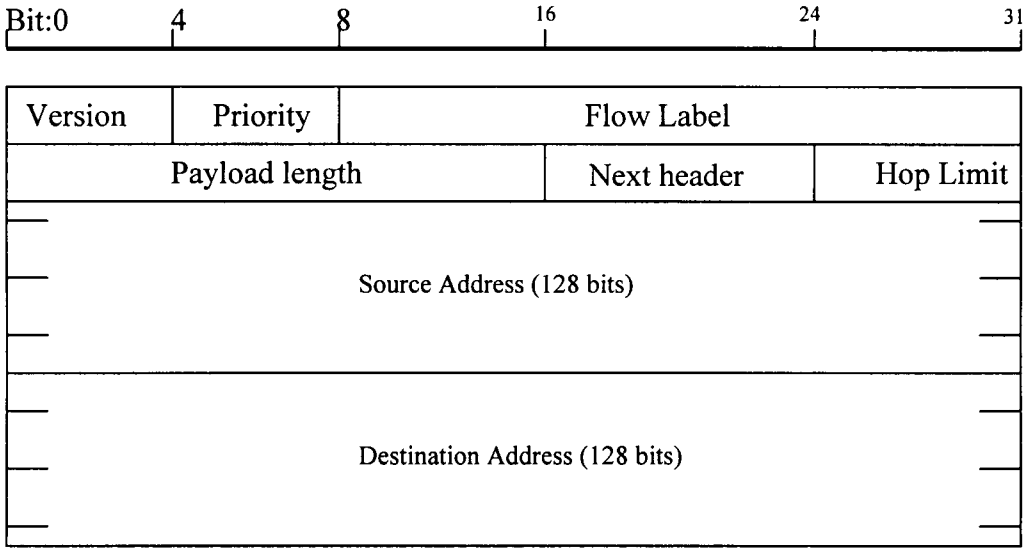


Figura 3.2 - Formato del encabezado del IPv6

ASPECTOS DE SEGURIDAD DEL IPv6

En el IPv6 es posible introducir un número arbitrario de encabezados (*headers*) de extensión entre el encabezado de Internet y el *payload*. Los diferentes tipos de encabezados (*headers*) se muestran en la tabla 3.1.

Tabla 3.1- Encabezados de extensión del IPv6

Hop by hop option header
Destination option header
Routing header
Fragment Header
Authentication header option header
Encapsulating Security payload header
Destination option header

- **Hop by Hop option header**. Lleva información que debe ser examinada y procesada por cada nodo en la trayectoria del paquete, con la fuente y el destino incluidos.
- **Routing Header**. Utilizado por una fuente para listar uno o más ruteadores que serán visitados por el paquete en su camino al destino.
- **Fragment Header.** Utilizado cuando la fragmentación es requerida. En el IPv6 la fragmentación solo puede hacerse en la fuente de la información.
- **Destination header.** Utilizado para llevar información que necesita ser examinada y procesada en el destino del paquete.
- **Authentication header y Encapsulated Security Payload header.**

Estos encabezados no son examinados por cada nodo que toque el paquete en su viaje, a excepción del encabezado de Hop-by-Hop, el cual si debe de ser revisado. Las especificaciones del IPv6 incluyen la descripción de dos *payloads* de seguridad.

El IPv6 nos ofrece con estos nuevos encabezados (headers) opciones de seguridad con las que no se contaba antes*: integridad, autenticación y confidencialidad.* Estas son aplicadas usando los nuevos encabezados, en particular el Authentication Header y el Encapsulated Security Payload *header*. A continuación se ven con un poco de más detalle.

AUTENTICACIÓN

La *autenticación* esta representada mediante un encabezado (*header*) opcional; la autenticación es un procedimiento mediante el cual el receptor del mensaje garantiza que la dirección de origen es autentica y que el paquete no ha sido alterado durante la transmisión. Esta operación consiste en la adición al datagrama del encabezado de autenticación (AH) y en la red, solo los nodos que se encuentran relacionados en la comunicación le pondrán atención a este encabezado extra. Los otros nodos simplemente lo ignoraran. Esto permite que los datagramas protegidos de esta manera, puedan ser capaces de viajar por redes que no usan el IPv6. La presencia del AH no cambia ni afecta el comportamiento de los protocolos de punto a punto como el UDP o el ICMP.

El AH cuida que no se cambie la información en nuestro paquete, esto lo hace calculando los **datos de autenticación** (AD) utilizando la información del datagrama que no cambia desde el envío hasta su destino. La información que se cambie es convertida a ceros. Para saber esto, la fuente del mensaje tiene que preparar un envío especial del paquete, cuya información sea independiente de transformaciones que puedan ocurrir en el tránsito. Después, es concatenada

una clave al principio y al final del paquete y se aplica una función *hash* (MD2 o MD5 por ejemplo) para procesar el mensaje, el resultado se llama **datos de autenticación** y se colocan dentro del AH.

Cuando el nodo destino recibe el paquete, este revisa el AH y verifica la validez del datagrama, este es aceptado solo si los datos de autenticación son correctos.

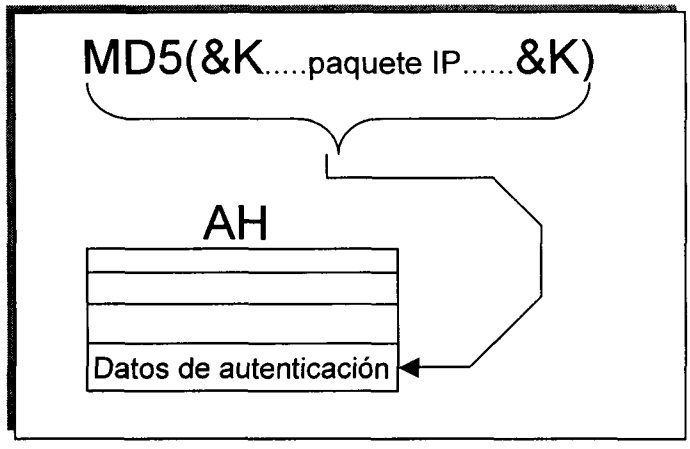


Figura 3.3 - Autenticación

ENCAPSULATED SECURITY PAYLOAD

El encabezado de *Encapsulated Security Payload* (ESP) garantiza que solo los receptores legítimos serán capaces de leer los paquetes. Este es el header a usar si se requiere confidencialidad. Aquí la carga computacional del cifrado es mayor que en el *authentication header*. El ESP esta fragmentado en dos partes, una es texto simple y la otra es texto cifrado. La parte del texto simple informa al nodo como procesar y desencriptar el ESP, la siguiente parte esta formada de campos protegidos y de texto cifrado.

El ESP (*Encapsulated Security Payload*) puede proveer de autenticación y encripción. ESP tiene dos modos: el modo de túnel y el modo de transporte. En el modo de túnel el paquete de IPv6 esta encapsulado en otro paquete IP de ESP.

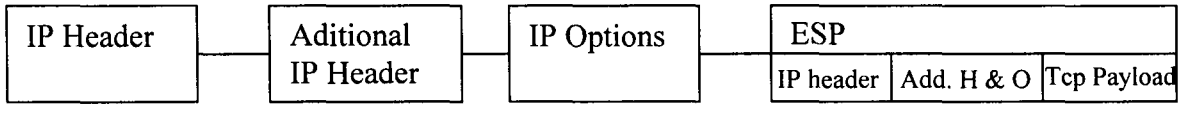


Figura 3.4 - ESP

En esta modalidad, el encargado del envío, toma todo el datagrama de IP y una vez que se determina la clave, el proceso de cifrado se realiza. Los datos cifrados son encapsulados dentro del *payload* del nuevo datagrama y así se transporta a su destino. El receptor deshecha el datagrama que envolvía al texto cifrado y una vez que la clave ha sido determinada descifra el *payload*. Cuando se utiliza el modo de túnel el verdadero encabezado del IP esta dentro del *payload* de IP y por lo tanto el intruso solo es capaz de ver las terminales de la línea asegurada. Si la línea asegurada existe entre dos firewalls, el observador solo puede ver que hay intercambio de

información entre las dos redes locales. Si este método de túnel seguro es colocado entre dos equipos de comunicación entonces el observador es solamente capaz de identificar a los comunicadores.

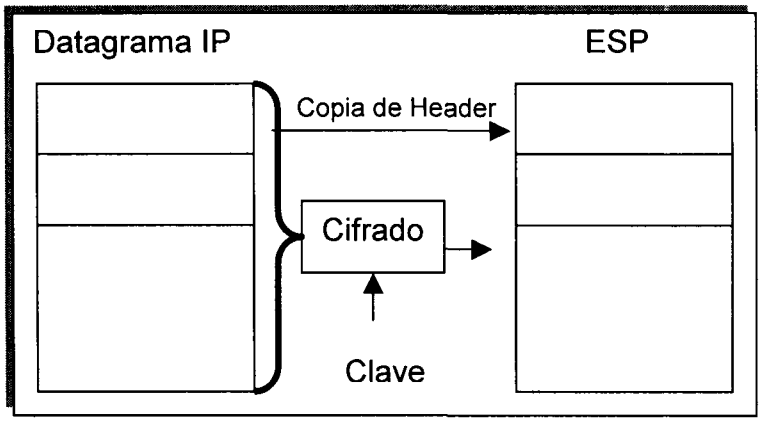


Figura 3.5 - ESP en modo túnel

En el modo de transporte no hay headers IP encriptados u opciones de IP de esta manera se ahorra ancho de banda. Es como se muestra en la figura 3.6:

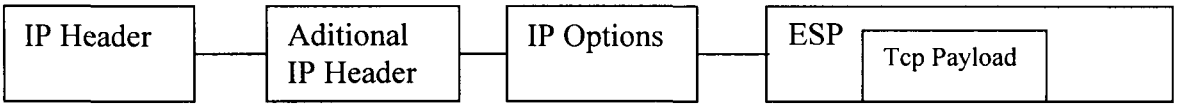


Figura 3.6 - ESP en modo transporte

En la modalidad de transporte se toma un paquete completo de la capa superior (TCP), el calculo se realiza con el mismo procedimiento descrito anteriormente, obteniendo un paquete de la capa de transporte cifrado dentro del ESP.

ESP y AH pueden ser usados de manera conjunta o independientes. Estos dos encabezados (headers) proveen de un servicio en el nivel de Internet. Si los servicios de seguridad son provistos en el nivel de Internet entonces serán fáciles de que otras aplicaciones los utilicen. Los protocolos como el RIP, OSPF o EL IDRP deben ser utilizados en altas asociaciones de seguridad entre los ruteadores con la finalidad de hacer imposible que se modifique el contenido de la tabla de ruteo.

Otro encabezado (header) que también se puede utilizar con fines de seguridad es el *Routing header* ya que con él se puede seleccionar la ruta deseada para así evitar que nuestra información pase por ruteadores o nodos que son agresivos y que pueden comprometer nuestros datos.

Utilizar el IPv6 también nos permite tener acceso al concepto de seguridad asociada. Bajo este concepto todos los protocolos de seguridad basados en el IPv6 o que usen las capacidades de este tendrán que ofrecer al menos una asociación de seguridad (SA). De esta manera, antes de usar el AH o el ESP los nodos que se encargaran de esta tarea, previamente deben acordar una SA que describa que parámetros de seguridad (funciones, modalidades, llaves) se van a usar. Sin embrago esto es parte de otro problema ya que para poder efectuar una correcta compartición del SA es necesario que la información que se manejara en común sea también enviada a través de un canal seguro o por medio de otro protocolo de seguridad, es decir que los nodos deben de tener una clave para intercambiar la información de SA, se necesita de un *Protocolo de*

Administración de Llaves. La IETF se encuentra trabajando en este asunto, pero no es tarea fácil, ya hay muchos trabajos en este problema: Photuris, Skip, y ISAKMP/Oakley. Con uno de los últimos trabajos siendo el ISAKMP/Oakley que después fue renombrado como IKE (Intercambio de Claves por Internet).El IKE se encarga de combinar el intercambio de llaves Diffie-Hellman con una autenticación subsiguiente de los parámetros de Diffie-Hellman.

Suponiendo que este sea el protocolo a usar para la transferencia de información, la negociación de una SA se lleva a cabo en dos partes, para comenzar el iniciador y el contestador acuerdan el uso de una llave en un canal seguro, esto incluye el intercambio de una "*cookie*" lo cual protege contra ataques del tipo de bloqueo de recursos. La primer fase es dedicada a establecer un canal seguro y autenticado entre las terminales, después de esto el iniciador y el receptor tienen que crear una nueva SA, la cual es llamada ISAKMP SA, que contiene los parámetros de seguridad que harán posible el intercambio de manera segura durante la fase 2 para la negociación de SA específicos. En la fase 2 es donde son negociadas las asociaciones especificas de seguridad en nombre de los servicios de IPsec o de cualquier otro que necesite un parámetro de negociación segura.

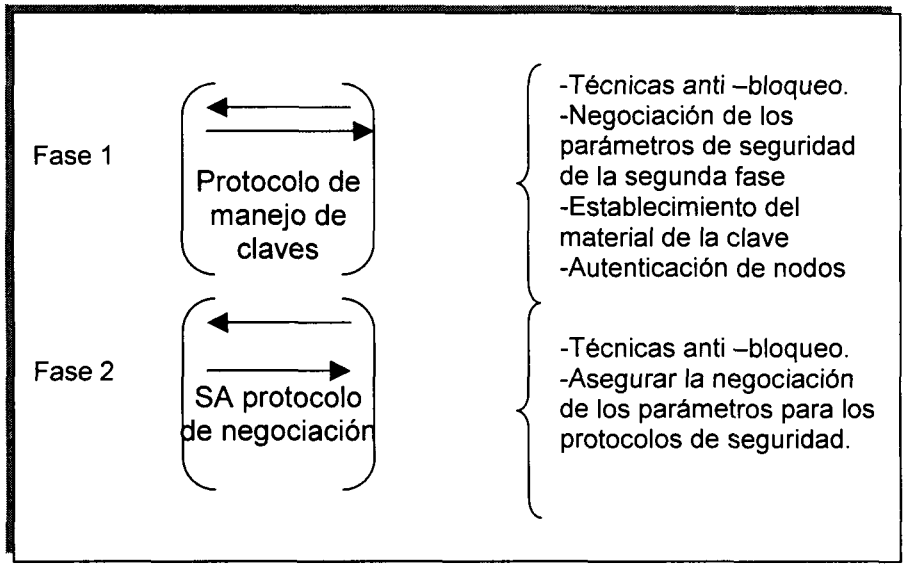


Figura 3.7 - Negociación de una SA

Los aspectos de seguridad que da el IPv6 nos abren toda una gama de posibilidades para tener una comunicación más segura.

- Líneas aseguradas y firewalls. El ESP y el AH del IPv6 nos permite crear una línea segura entre dos firewalls distantes, por ejemplo entre dos unidades de una misma organización.
- Hosts móviles. Una manera de evitar los ataques específicos a computadoras móviles es establecer un túnel seguro entre el equipo móvil y el firewall de la red.
- Protocolos de ruteo. La integridad de la red no puede ser mantenida si los protocolos de ruteo no son asegurados. Si los intrusos son capaces de acceder a las actualizaciones de ruteadores entonces serán capaces de desviar o tergiversar la información.
- Estación de trabajo a estación de trabajo. La conexión segura se establece entre dos hosts que estén en LANs distintas e interconectadas por medio de un enlace de firewall-a-firewall.

SSL & TLS
Secure Socket Layer & Transport Layer Secure

Secure Socket Layer es el protocolo de seguridad de Internet para conexiones punto-a-punto. Desarrollado por Netscape, es utilizado por exploradores de Internet y servidores de Red. Ofrece protección contra incursiones, forjado o el *tampering*. Clientes y servidores son capaces de autentificarse uno al otro y establecer un enlace seguro o "tubería" que atraviesa la Internet o una red local para que los datos sean transferidos de manera segura.[24]

En nuestro explorador podemos ver si estamos usando un protocolo de seguridad tal como TLS en diferentes maneras. Se puede apreciar en la línea de dirección es reemplazada con las iniciales "https" y también con un pequeño candado en la barra de estado en la parte de abajo del explorador. En la figura 3.8 se ve un ejemplo.

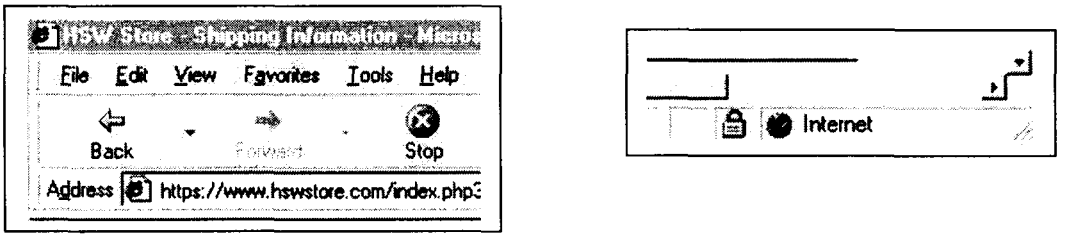


Figura 3.8 - Seguridad en el explorador

El protocolo SSL es análogo a una llamada telefónica en una línea segura entre dos computadoras en cualquier red incluyendo la Internet. En SSL la conexión es establecida, las partes autenticadas y la información transferida con seguridad. A la última mejora de este protocolo se le llamó TLS.

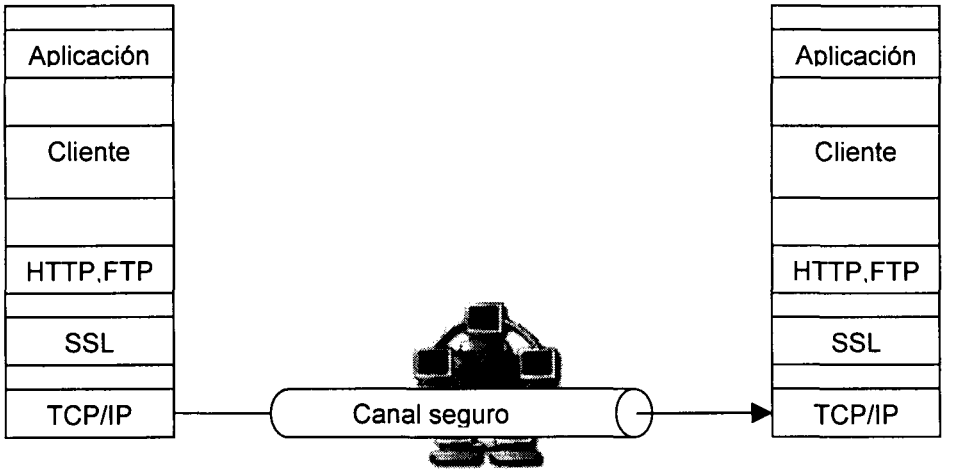


Figura 3.9 - Conexión SSL

En aplicaciones utilizando SSL, se utilizan fuertes medidas de encripción para asegurar la confidencialidad. Por medio del uso de certificados digitales, SSL provee de la autentificación transparente de servidores y de manera opcional, de los clientes. SSL utiliza el algoritmo **RSA**

como el algoritmo encargado de manejar la seguridad utilizando firmas digitales y sobres digitales. Para una encripción y desencripción para una transferencia de datos muy rápidos después de que una conexión SSL ha sido establecida, se recomienda el uso del algoritmo **RC4.**

SSL es utilizada en la Red para muchas aplicaciones. Si una terminal de la conexión no esta habilitada para SSL o para la Red, entonces se necesitan herramientas para construir SSL en esta aplicación. Otras situaciones requieren que las aplicaciones tengan más control sobre las conexiones incluyendo la selección de plataformas de cifrado y de negociación de llaves. Los desarrolladores que utilizan el SSL incluido en el explorador de Red tienen muy poco control sobre el desempeño y operación de SSL

SSL opera en la capa de transporte, abstraído de la capa de red, donde opera IPsec, SSL opera entre dos aplicaciones cualesquiera que no necesariamente tienen que estar en la misma red segura. SSL se encarga de asegurar dos aplicaciones mientras que IPsec se encarga de asegurar toda una red. Las aplicaciones de SSL son muy variadas ya que puede utilizarse prácticamente donde sea necesario un enlace protegido entre dos computadoras o aplicaciones. SSL en el explorador de la Red no basta para asegurar la mayoría de los sistemas. Los sistemas tales como el acceso a una base de datos segura o sistemas remotos de objetos tales como Corba puede asegurarse mediante el uso de SSL. Los bancos también pueden emplear SSL para comunicarse con sucursales remotas empleando una fuerte criptografía. Otra aplicación de SSL es para crear acceso remoto a aplicaciones administrativas.

S/MIME
Secure Multipurpose Internet Mail Extensions

S/MIME es el protocolo encargado de ofrecer la privacidad necesaria a los negocios electrónicos de la Red, ofreciendo los servicios de autenticidad y privacidad. S/MIME utiliza la encripción por llave pública para evitar que los mensajes sean interceptados o reforjados. La analogía de la protección ofrecida por S/MIME es de un correo postal enviado entre dos lugares de manera segura. El protocolo garantiza la aseguración del mensaje, la autenticación, el almacenamiento y la transmisión de los datos secretos.

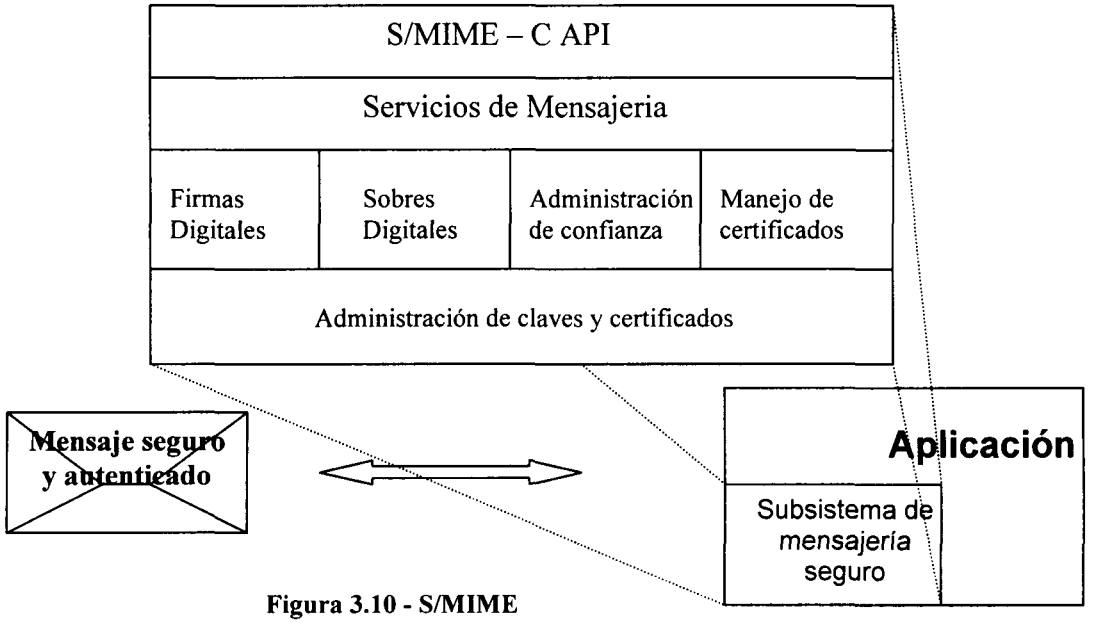


Figura 3.10 - S/MIME

Los protocolos tales como el SSL y TLS se encargan de la protección a un nivel de aplicación para que dos equipos se conecten de manera segura en una red pública, mientras que otros protocolos, como el IPsec, mantienen la seguridad a un nivel más bajo, en las comunicaciones de la red. Sin embargo, estos protocolos no ofrecen seguridad para el almacenamiento o la transmisión de los datos. Es aquí donde se aplica S/MIME.

S/MIME esta basado en el algoritmo RSA para la utilización de firmas digitales y sobres digitales. Los algoritmos RC2, DES y Triple DES son utilizados para encripción simétrica. Para utilizar las funciones hash, S/MIME se basa en el uso de MD5 y el SHA1.

Las aplicaciones de S/MIME son muy variadas, ya que se puede usar siempre que se quiere almacenar, transmitir y autenticar datos o mensajes importantes. Por ejemplo, las formas de los bancos, recibos de pagos, estados de cuenta, hipotecas, pagos en línea, los clientes que utilizan aplicaciones con S/MIME confiadamente pueden pagar sus cuentas o hacer compras con tarjeta de crédito, incluso en aplicaciones medicas ya que se pueden guardar los registros de los pacientes.

IPsec
IP Security Protocol

IPsec es el protocolo estándar para la aplicación de confidencialidad, autenticación e integridad en la capa del datagrama de IP. IPsec comprende la base para la interoperabilidad de "tuberías" aseguradas de terminal-a-terminal, túneles encapsulados y Redes Privadas Virtuales (VPNs), con lo que se provee protección para los protocolos cliente que residen sobre la capa de IP. IPsec se encarga de asegurar que los datos enviados por una red segura estén íntegros y que no hayan sido corrompidos por atacantes.

En la capa de IP, las computadoras en la red se comunican por medio del ruteo de paquetes o datagramas. En una red local estos datagramas no tienen ningún método de protección por lo que son muy fáciles de alterar por intrusos. Normalmente esto se evita mediante el uso de los firewalls, sin embargo en Internet es muy difícil evitar que nuestros datagramas sean interceptados y alterados.

IPsec esta basado en el algoritmo Diffie-Hellman y el algoritmo RSA para el intercambio de llaves. Para la encripción simétrica, los algoritmos DES y Triple DES son utilizados. En situaciones donde mayor seguridad es requerida para encripción en IPsec, el algoritmo RC5 es utilizado comúnmente. Para las funciones *hash*, se utilizan SHA1 y MD5. IPsec mantiene seguros los paquetes en la red de bajo nivel para poder crear una red segura de computadoras sobre canales inseguros, incluyendo en Internet.

IPsec es aplicable en cualquier situación en la que se desea comunicación entre redes seguras. Muchas organizaciones usan el IPsec estándar para construir software que habilita VPNs, con esto se pueden crear redes seguras sobre redes inseguras. Usando VPNs las compañías se pueden ahorrar el dinero de instalar líneas dedicadas y mantener la confidencialidad de la información corporativa. Software de acceso remoto basado en el estándar de IPsec provee a las empresas de accesos seguros a sus funciones de redes. Los firewalls pueden fácilmente incorporar IPsec para crear un túnel con una red VPN, esto permite que las empresas hagan enlaces con sus compañeros de negocios o clientes y que se sigan manteniendo la integridad de las comunicaciones.

En la tabla 3.2 mostramos los principales protocolos de seguridad y sus características:

Tabla 3.2 - Principales protocolos de seguridad

PROTOCOLO	DETALLES	ALGORITMOS QUE USA
CDPD (Cellular Digital Packet Data)	Estándar diseñado para habilitar a los clientes el envió de datos de computadora sobre redes celulares	Diffie-Hellman RC4
DNSSEC (Domain Name System Security Extensions)	Protocolo para servicios de nombre distribuidos tales como nombre de *host* y búsqueda de dirección de IP	RSA MD5 DSA
IEEE 802.11	Protocolo estándar para productos inalámbricos de LAN	RC4 MD5
SSH (Secure Shell)	Protocolo que permite usar acceso remoto seguro sobre una red de una computadora a otra	RSA RC5 RC4 RC2 DES 3DES
SET (Secure Electronic Transactions)	Permite transacciones seguras de tarjetas de crédito en Internet	RSA SHA1 DES HMAC-SHA1
PPTP (Point-to-Point Tunneling Protocol)	Usado para crear comunicación entre VPNs por medio de la Internet, trabaja en la capa de datagrama de IP	RSA DES
DOCSIS (Data Over Cable Service Interface Specification)	Estándar de modem de cable para la transmisión segura de datos con protección contra ataques de robo de servicio y negación de servicio	RSA DES HMAC SHA1

CAPITULO 4

RECOMENDACIONES DE SEGURIDAD Y PRUEBAS DE ENCRIPCION

Con el objetivo de comprender claramente la importancia de la seguridad en un sistema de información o computacional, se hizo la recopilación de información presentada en los capítulos anteriores acerca de cuáles son los elementos que podrían constituir fallas o posiciones que no otorgan o comprenden un nivel aceptable de seguridad informática para las distintas aplicaciones que se manejan hoy en día, así como las principales vulnerabilidades que afectan a los distintos sistemas operativos con mayor cantidad de usuarios.

El presente capítulo, muestra los resultados de la investigación en herramientas de seguridad y criptografía, por ello esta dividido en tres partes principales. En la primer parte se hacen recomendaciones de seguridad para los sistemas operativos Windows, UNIX, LINUX y Solaris. En la segunda parte las recomendaciones son para distintas configuraciones de sistemas computacionales, otorgándoles una calificación o rating al nivel de seguridad del sistema antes y después de hacer las recomendaciones. Para la tercer parte se presentan las pruebas de encripción realizadas con algoritmos implementados en MAPLE y con programas de encripción provenientes de Internet.

VULNERABILIDADES Y RECOMENDACIONES DE SEGURIDAD EN SISTEMAS OPERATIVOS

El éxito en los ataques a los sistemas operativos se debe en su mayor parte al aprovechamiento de unas pocas vulnerabilidades del software utilizado. Los atacantes son siempre oportunistas y por lo general explotan las fallas más conocidas con las herramientas que estén disponibles. Muchos de los ataques computacionales, como se ha mencionado en capítulos anteriores, se basan en aprovechar que las organizaciones no reparan las vulnerabilidades con parches informáticos ya existentes.

La reparación de vulnerabilidades no se lleva a cabo por diversas razones, como el no saber cuales son las más riesgosas, la cantidad de trabajo no permite su solución, o no hay conocimiento de cómo arreglarlas de una manera segura. Además que si se aplica un scanner de riesgos a un sistema o computadora el número de vulnerabilidades puede alcanzar cantidades de dos mil, y eso impresiona a cualquiera. Sin embargo, muchas de estas fallas pueden repararse al actualizar el sistema o descargar los parches necesarios. Sería muy difícil mencionar todas las versiones existentes sistemas de operativos, por ello, la finalidad es que este documento sea de utilidad para todo aquel que desee iniciarse en la seguridad informática y sirva de base en las decisiones para comenzar a proteger los sistemas. A continuación se describen a detalle las principales vulnerabilidades de cada sistema operativo, y se proponen soluciones para estos problemas de seguridad.

SISTEMA MICROSOFT WINDOWS

Para hacer un recuento de las principales vulnerabilidades que se pueden explotar en el sistema operativo Windows de Microsoft, nos basamos en una investigación y recolección realizadas
por el Instituto SANS y la Agencia Federal de Investigación de los Estados Unidos (FBI). [26]

1. **Servicios de Información de Internet (IIS)**. IIS presenta vulnerabilidades de tres clases principales: incapacidad para manejar peticiones no anticipadas, desbordamientos de buffer y aplicaciones de muestra.
    - *Incapacidad de Manejar Peticiones no Anticipadas.* Muchas de las vulnerabilidades de IIS están relacionadas con la incapacidad de manejar peticiones HTTP formadas impropiamente. Un buen ejemplo es la vulnerabilidad *Unicode directory traversal* explotada por el gusano (*worm*) Code Blue. Si se arma una petición que explote una de estas vulnerabilidades, un atacante remoto puede hacer lo siguiente: Ver el código fuente de las aplicaciones utilizadas, ver los archivos fuera de la raíz de documentos Web, ver los archivos que el servidor de Internet ha sido instruido para no servir, ejecutar comandos arbitrarios en el servidor para borrar archivos o instalar una puerta trasera.
    - *Desbordamientos del Buffer.* Muchas extensiones ISAPI; tales como ASP, HTR, IDQ, PRINTER, SSI; son vulnerables a desbordamientos de buffer. Un ejemplo es la vulnerabilidad de la extensión ISAPI ***.idq***, la cual fue aprovechada por los gusanos Code Red y Code Red II. Una petición cuidadosamente creada de un atacante remoto puede resultar en lo siguiente: Negación de servicio, ejecución arbitraria de código o comandos en el contexto del usuario de servidor de Internet.
    - *Aplicaciones de Muestra.* Las aplicaciones de muestra son generalmente diseñadas para demostrar la funcionalidad del ambiente de un servidor, no para resistir ataques, y no están planeadas para que sirvan como aplicaciones de producción. El problema es que su localización por default es conocida y su código fuente disponible a escrutinio, esto las hace blancos de intentos de explotación. Las consecuencias pueden ser severas: Una aplicación de muestra, tal como ***newdsn.exe***, le permite a un atacante remoto crear o sobrescribir archivos en el servidor.

    Los sistemas operativos afectados por las vulnerabilidades de IIS son Windows NT 4 corriendo IIS 4, Windows 2000 Server corriendo IIS 5, Windows XP Profesional corriendo IIS 5.1. Para estar protegido contra esta vulnerabilidad se recomienda:
    - Aplicar los parches informaticos mas actuales. Para el caso de usar IIS 4 sobre NT4 con Service Pack 6, hay que aplicar un paquete de actualizacion de seguridad acumulado e individualmente un parche. En el caso de usar IIS 5 o 5.1 sobre Windows 2000 o XP, el parche y el acumulado están incluidos en el paquete de servicio.
    - Seguir estando pendiente de nuevas vulnerabilidades que aparezcan y de los correspondientes parches. HFNetChk (Network Security Hotfix Checker) es un programa que asiste al administrador del sistema y revisa sistemas locales y remotos para encontrar parches nuevos, este programa funciona en Windows NT4, Windows 2000, Windows XP y puede ser descargado del sitio de Microsoft en Internet.
    - Eliminar las aplicaciones de muestra. Las aplicaciones de muestra, incluyendo la herramienta ***iisadmin*** puede ser usada para revisar que la instalación del servidor fue correcta, pero debe ser eliminada inmediatamente.
    - Deshacer el mapa de extensiones ISAPI no necesarias. La mayoría de los desplegados IIS no tienen necesidad para la mayoría de las extensiones ISAPI que son mapeadas por default como ***.htr, .idq, .ism*** y ***.printer***.

- Filtrar las peticiones http. Muchas explotaciones de IIS, incluyendo las de la familia de Code Blue y Code Red, utilizan peticiones http maliciosamente formadas en ataques de sobreflujo de buffer. El filtro URLScan puede ser configurado para rechazar tales peticiones antes de que el servidor intente procesarlas. Esta herramienta puede ser descargada del sitio de Microsoft.

2. **Componentes de Acceso a Datos Microsoft (MDAC).** El componente de Servicios de Datos Remotos en versiones viejas de MDAC tiene una falla de programa que permite a usuarios remotos ejecutar comandos localmente con privilegios administrativos. Si se combina con la falla en el motor de bases de datos 3.5 Microsoft Jet, pueden proveerse de accesos anónimos externos a bases de datos internas. Estas fallas están bien documentadas y las soluciones han estado disponibles por mas de dos años, sin embargo los sistemas viejos o mal configurados siguen estando expuestos o sujetos a ataques.
   Los sistemas operativos y programas afectados por la vulnerabilidad de MDAC son Windows NT 4.0 corriendo IIS3.0 o 4.0, Servicios de Datos Remotos 1.5, o el Visual Studio 6.0. Para protegerse de esta vulnerabilidad se puede descargar una guía para las debilidades RDS y Jet del sitio ***www.wiretrip.net***. Además, Microsoft ha liberado varios boletines de seguridad detallando este problema y la forma de repararlo vía ciertos cambios de configuración, y están disponibles en el sitio de Internet de Microsoft. Para prevenir que ocurra este problema se recomienda también instalar la versión MDAC 2.1 o superior, las versiones más recientes de MDAC están disponibles en la página en línea de Microsoft.

3. **Servidor Microsoft SQL**. El Servidor Microsoft SQL (MSSQL) contiene varias vulnerabilidades serias que permiten a atacantes remotos obtener información sensible, alterar el contenido de bases de datos, comprometer la seguridad de servidores SQL, y en algunas configuraciones comprometer a servidores anfitriones.
   Las vulnerabilidades de MSSQL son muy conocidas y están activamente usándose para atacar. Recientemente, en Mayo de 2002 y Enero de 2003 dos gusanos de MSSQL explotaron varias fallas conocidas de MSSQL. Los servidores anfitriones atacados por estos gusanos generaron un nivel perjudicial de trafico en la red al hacer una búsqueda de otros servidores vulnerables.
   Uno de los gusanos que exploto estas vulnerabilidades, el SQLSnake, su rutina depende de la cuenta administrativa por default, que tiene un password vacía. Es esencial para la correcta configuración y defensa de cualquier sistema asegurarse que todas las cuentas del sistema estén protegidas por password o completamente deshabilitadas si no se usan.
   El gusano SQL Slammer tiene una rutina de ataque la cual consta en un desbordamiento del buffer del Servicio de Resolución de Servidor SQL. Este desbordamiento causa que la seguridad del anfitrión sea comprometida cuando el gusano envía paquetes de ataque al puerto UDP 1434 de sistemas vulnerables. Si una máquina corre servicios SQL que son sujetos a este desbordamiento de pila de buffer y recibe paquetes de esta naturaleza, generalmente resultara en que la seguridad del servidor y del sistema han sido comprometidos totalmente.
   El Motor de Escritorio de Servidor Microsoft 2000 (MSDE 2000) puede entenderse que es un "Servidor SQL Ligero". Muchos propietarios de sistemas no se dan cuenta que sus sistemas corren MSDE y que tienen una versión del Servidor SQL instalada. MSDE 2000 es instalada en los siguientes productos de Microsoft:
   - Servidor SQL/MSDE 2000
   - Visual Studio .Net
   - ASP.NET Herramienta de Matriz de Red
   - Office XP
   - Access 2002
   - Visual Fox Pro 7.0/8.0

MSDE 2000 puede configurarse para "escuchar" las conexiones de entrada de clientes en diferentes maneras. De igual manera puede ser configurado para que los clientes puedan usar ciertas tuberías nombradas sobre una sesión de NetBIOS (puerto TCP 139/445) o los *sockets* con clientes conectados al puerto TCP 1433. Cualquier método que se use, el Servidor SQL y MSDE siempre escucharan el puerto UDP 1434. Este es denominado como el puerto monitor. Los clientes enviaran un mensaje a este puerto para descubrir dinámicamente como debe conectarse el cliente al servidor. Cuando se le presenta un paquete 0x02 de un solo byte en el puerto UDP 1434, el motor MSDE 2000 regresa información acerca de sí mismo. Este tipo de ataques se ven exacerbados si son canalizados sobre UDP. Ya sea que el proceso MSDE 2000 corra en el contexto de seguridad de un usuario de dominio o de la cuenta del sistema local, una explotación exitosa de estos agujeros en seguridad puede significar una puesta en riesgo de la totalidad del sistema.

Los sistemas operativos que están en riesgo por esta vulnerabilidad en MSSQL son cualquier sistema Windows con Microsoft SQL/MSDE Servidor 7.0, Microsoft SQL/MSDE Servidor 2000 ó Microsoft SQL/MSDE Server Desktop Engine 2000 instalado, al igual que cualquier sistema que use el motor MSDE por separado. Para solucionar los problemas causados por esta vulnerabilidad se pueden tomar en cuenta las siguientes recomendaciones:

- Deshabilitar el monitor del servidor SQL/MSDE en el puerto UDP 1434. Esto puede llevarse a cabo instalando y usando las funciones dentro del paquete de servicio Servidor SQL 2000.
- Aplicar los más nuevos paquetes de servicio para el servidor Microsoft SQL/MSDE y para MSDE 2000r.
- Aplicar el parche acumulado más reciente después de instalar un nuevo paquete de servicio.
- Aplicar cualquier parche individual que sea liberado después del nuevo parche acumulado.
- Habilitar la autenticación de acceso del Servidor SQL. Comúnmente esta opción no esta habilitada. Esto se hace en el menú de *Enterprise Manager*.
- Asegurar el servidor a nivel sistema y red. Se debe seguir la recomendación del tema "Acceso del Administrador del Sistema" en los libros en línea del Servidor SQL/MSDE para asegurarse que la cuenta "**sa**" (administrador del sistema) tenga un password resistente.
- Minimizar los privilegios para el servicio del Servidor MSSQL/MSDE y del agente del Servidor SQL/MSDE.

4. **NETBIOS**. Windows de Microsoft provee una máquina anfitriona con la habilidad de compartir archivos o carpetas a través de una red con otros anfitriones con las capacidades de red de Windows. La base de este mecanismo es el protocolo Servidor de Bloques de Mensaje (SMB), o el Sistema de Archivos Comunes por Internet (CIFS). Estos protocolos le permiten a un anfitrión manipular archivos remotos como si fueran locales.

   Aunque este es una característica importante y poderosa de Windows, una configuración impropia de los archivos compartidos en red puede exponer sistemas de archivos críticos o puede proveer un mecanismo para que un usuario o programa malicioso tomen control total de un anfitrión. Una de las maneras en que el virus Sircam y el gusano Nimda se esparcieron tan rápido en el verano del 2001 fue al descubrir uso compartido de red no protegidas y colocando una copia de sí mismos en estas redes. Muchos propietarios de computadoras sin saberlo abren sus sistemas a piratas cuando intentan mejorar la accesibilidad para compañeros del trabajo haciendo sus unidades de disco puedan ser leídas y modificadas por usuarios de red. Si se hace una correcta configuración de las opciones de archivos compartidos en la red, los riesgos de comprometer el sistema son mitigados.

Los sistemas operativos que podemos encontrar siendo afectados por las vulnerabilidades de NETBIOS son: Windows 95, Windows 98, Windows NT, Windows 2000, Windows Me y Windows XP. Para protegerse de esta vulnerabilidad, las recomendaciones son:

- Deshabilitar compartir siempre que no sea requerido. Si debe cerrarse un aspecto compartido, se puede hacer a través del menú propiedades del explorador de Windows para ese directorio, en Administrador del Servidor para Dominios o en Editor de Políticas de Grupo.
- No permitir compartir archivos con anfitriones en Internet.
- No permitir la compartición sin autenticación.
- Restringir la compartición a solo el mínimo de carpetas requeridas.
- Restringir permisos en carpetas compartidas al mínimo requerido.
- Para mayor seguridad, permitir compartir solo con direcciones especificas ya que los nombres DNS pueden ser falsificados.
- Bloquear los puertos usados para comparticiones Windows en el perímetro de la red. Bloquear los puertos del NetBIOS comúnmente usados por Windows en el perímetro de la red usando un ruteador externo o un firewall de perímetro.

5. **Acceso de Usuarios Anónimo**. Una conexión de sesión nula, también conocida como Acceso de Usuario Anónimo, es un mecanismo que permite a un usuario anónimo extraer información (como nombres de usuario y compartidos) por medio de la red, o conectarse sin autenticación. Es utilizado por aplicaciones como el Explorador de Windows para enumerar los compartidos en servidores remotos. En Windows NT, 2000 y sistemas XP, hay servicios locales que corren bajo la cuenta de SISTEMA, que se conoce como LocalSystem en Windows 2000 y XP. La cuenta de SISTEMA es usada para varias operaciones criticas del sistema. Cuando una máquina necesita extraer información del sistema de datos de otra, la cuenta de SISTEMA abrirá una sesión nula hacia la otra máquina.
   La cuenta de SISTEMA tiene privilegios virtualmente ilimitados y sin password, de manera que no puedes acceder haciéndote pasar por SISTEMA. Pero SISTEMA a veces necesita acceder información en otras máquinas, tales como compartidos disponibles, nombres de usuarios, etc. Es decir las clásicas funcionalidades ofrecidas por el entorno de red. El problema en sí, es que SISTEMA no accesa a otros sistemas usando una cuenta de usuario y password, sino que usa una sesión nula. Desafortunadamente los atacantes pueden también ingresar en forma de una sesión nula.
   Los sistemas operativos vulnerables a estos ataques son: todas las versiones de Microsoft Windows NT, 2000 y XP. Con la finalidad de evitar este ataque se debe tener en cuenta que los controles de dominio requieren sesiones *Null* para comunicarse. Por ello, si se trabaja en un ambiente de dominio, se puede minimizar la información que los atacantes pueden obtener, aunque no se puede detener toda la fuga. Para limitar la información disponible a los atacantes, se puede modificar la clave siguiente de registro:
   HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=1
   Se puede modificar el registro, pero puede causar que el sistema deje de trabajar correctamente. Al colocar RestrictAnonymous en 1 se minimiza la fuga, esto es para NT. Para los sistemas Windows 2000 y XP se coloca el valor en 2., pero ello puede afectar la sincronización del dominio u otros servicios, por ello mismo se recomienda que solo aquellas maquinas visibles a Internet tengan configurado este valor. Todas las otras máquinas deben ser protegidas con un firewall configurado para bloquear NetBIOS y CIFS. En caso de no necesitar compartir carpetas o servicios de impresión se recomienda separar NetBIOS de TCP/IP.

6. **Autenticación de administrador de LAN**. Aun y cuando la mayoría de los ambientes Windows actuales no necesitan un soporte para administrador de LAN (LM), Microsoft almacena de forma local versiones modificadas mediante funciones *hash* de passwords

para LM en los sistemas Windows NT, 2000 y XP. Debido a que LM utiliza un esquema de encripción mucho más débil que la mayoría de los métodos actuales de Microsoft (por ejemplo el Administrador de LAN NT y el Administrador de LAN NT 2), los passwords de LM pueden ser rotas en un periodo de tiempo muy corto. Incluso passwords que de otra manera se considerarían "resistentes" pueden ser decodificadas por la fuerza en menos de una semana con el hardware actual.

La debilidad de las versiones *hash* de passwords de LM se deriva por las siguientes razones:

- Los passwords son truncadas en 14 caracteres.
- Passwords son rellenadas con espacios para ser de 14 caracteres.
- Passwords son todas convertidas a mayúsculas
- Passwords son divididas en dos conjuntos de siete caracteres.

El proceso de aplicar funciones *hash* hace posible que un atacante necesite solo de completar la trivial tarea de descubrir dos passwords de siete caracteres que se sabe están en mayúsculas, y así obtener acceso autenticado al sistema. La complejidad de descubrir valores *hash* se incrementa geométricamente con la longitud de estos. Cada una de las cadenas de siete caracteres es más simple de atacar por lo menos en un orden de magnitud de lo que seria efectuar un ataque a una cadena de catorce caracteres. Como todas las cadenas son de siete caracteres exactamente, incluyendo espacios y completamente en mayúsculas, un ataque estilo diccionario se simplifica. El método *hash* para LM ignora completamente buenas políticas de password.

Además del problema anteriormente expuesto, el proceso de autenticación del administrador de LAN es frecuentemente habilitado por default en clientes y aceptado por servidores. Como resultado, máquinas con Windows capaces de utilizar algoritmos *hash* más resistentes envían débiles valores hash de LM a través de la red, haciendo la autenticación de Windows vulnerable a actividades de "escucha" (*eavesdropping*) al hacer una revisión de paquetes. Con lo cual se facilitan los esfuerzos de un atacante para obtener y descifrar passwords de usuario.

Los sistemas operativos afectados por esta vulnerabilidad son todas las versiones de Windows. Para proteger el sistema de esta falla se recomienda:

- Deshabilitar autenticación del administrador de LAN (*LM Authentication*) a través de la red. El mejor reemplazo en Windows para la autenticación del *Lan Manager* es el programa *NT Lan Manager versión 2*. Los métodos de desafío/respuesta del NTLMv2 superan muchas de las debilidades en *Lan Manager* al utilizar encripción más resistente y una autenticación mejorada.
- Evitar que el valor *hash* de *Lan Manager* sea almacenado. Un gran problema con el borrado de los *hashes* de *Lan Manager* que circulan por la red local es que los *hashes* son aun creados y almacenados en el SAM o Directorio Activo. Microsoft tiene un mecanismo disponible para apagar la creación de *hashes* de *Lan Manager*, pero solamente en Windows 2000 y XP.

7. **Autenticación General de Windows**. Las palabras de pase, frases de pase y códigos de seguridad son usadas en casi cualquier interacción entre usuarios y sistemas de información. La mayor parte de autenticación de usuarios, al igual que la protección de datos y archivos, se basan en passwords dadas por usuarios. Un password comprometido da la oportunidad de explorar un sistema desde su interior sin ser detectado, ya que si se entra de manera legal y autenticada no es probable que se levanten sospechas. Así, un atacante tendrá acceso completo a los recursos disponibles para este usuario, y estará significativamente cerca de poder accesar otras cuentas, máquinas cercanas, y quizás hasta privilegios administrativos. A pesar de estos riesgos, las cuentas con malas o vacías passwords siguen siendo muy comunes, y las organizaciones con buenas políticas de passwords siguen siendo muy raras.

   Las vulnerabilidades de password más comunes son:

a) Cuentas de usuario que tienen passwords débiles o que simplemente no tienen password.
b) A pesar de la fortaleza de su password, los usuarios fallan en mantenerla secreta.
c) El sistema operativo o el software adicional crea cuentas administrativas con paswords débiles o sin ellas.
d) Los algoritmos *hash* para password son conocidos y frecuentemente los valores *hash* son almacenados, de manera que son visibles por cualquiera.

La mejor defensa contra esto es tener una fuerte política de password la cual incluya instrucciones completas para buenos hábitos con passwords y una revisión proactiva de su integridad.

Todos los sistemas operativos o aplicaciones en donde los usuarios usen autenticación por medio de un ID y password son débiles ante esta vulnerabilidad. Para defender el sistema contra esta amenaza se puede aplicar una política fuerte la cual incluya instrucciones precisas con la finalidad de engendrar buenos hábitos de passwords y una revisión proactiva de la integridad de passwords. Como encargado de la seguridad, uno se debe asegurar que los passwords sean resistentes, ya que con suficiente hardware y tiempo cualquier password puede ser descubierto por métodos de fuerza bruta. Las recomendaciones en cuanto a la creación de password se verán mas adelante con mas detalle para cada configuración de sistemas. El administrador del sistema, puede usar herramientas para descifrar passwords si antes se obtienen los permisos necesarios, con la finalidad de indicarle a los usuarios de una red si deben de cambiar por un password mas seguro. Si los problemas con el uso de passwords son muchos entonces se puede optar por utilizar medidas biométricas de autenticación, tal y como se explica mas adelante en la sección de ***controles físicos*** de las configuraciones de sistemas. También se debe mantener una lista maestra de las cuentas de usuarios con la cual hacer auditorias de seguridad, sin olvidar los passwords para los ruteadores, impresoras conectadas a Internet, copiadoras y controladores de impresoras, y tener la capacidad de borrar las cuentas cuando ya no estén en uso y de incluir nuevas cuentas autorizadas. El administrador de seguridad debe diseñar rigurosos procedimientos para remover las cuentas cuando los empleados o los contratistas sean despedidos y que sus cuentas no sean necesarias. Existen herramientas disponibles para ayudar con una buena política de passwords, por ejemplo ***Symantec Enterprise Security Manager*** (ESM) permite el monitoreo de cualquier cambio en políticas, creación de nuevas cuentas y resistencia de passwords. ESM intentara descifrar passwords mientras desempeña la ejecución de políticas en la red. ESM monitorea los registros de accesos y cualquier cambio que haya sido hecho a la estructura de la red.

8. **Internet Explorer**. Microsoft Internet Explorer es el navegador de la red por default instalado en las plataformas de Microsoft Windows. Todas las versiones existentes de Internet Explorer tienen vulnerabilidades criticas. Un administrador de red malicioso puede diseñar páginas para explotar estas vulnerabilidades mientras se navega por la página.
Las vulnerabilidades pueden ser categorizadas en múltiples clases incluyendo falsificación (*spoofing*) de páginas web, vulnerabilidades de control *Active*, vulnerabilidades de alteraciones *Active*, mala interpretación del tipo MIME y del tipo contenido, y desbordamiento de buffer. Las consecuencias pueden incluir la apertura de cookies, archivos locales o datos, ejecución de programas locales, descarga y ejecución de código arbitrario o una toma del control del sistema vulnerable.
Estas vulnerabilidades existen en los sistemas Windows de Microsoft que utilicen cualquier versión del Microsoft Internet Explorer. Es importante hacer notar que IE es instalado con una amplia variedad del software de Microsoft, y por lo tanto, esta presente en todos los sistemas Windows, incluso en servidores donde la navegación es raramente necesaria. Para proteger nuestro sistema contra amenazas por esta vulnerabilidad se pueden aplicar parches informáticos que están disponibles para las versiones 5.01, 5.5 y 6.0 en la página

en línea de Microsoft. Si el sistema tiene una versión anterior a estas del Internet Explorer se debe instalar la actualización y después los parches de seguridad ya sean de manera individual o instalando los paquetes acumulados. Para mantener la protección del sistema, hay que estar pendiente de cualquier nueva actualización de Internet Explorer por medio de *Windows Update, HFNetChk,* o de *Microsoft Baseline Security Analyzer (MBSA).*

9. **Acceso Remoto al Registro**. Windows 9x, Windows CE, Windows NT, Windows 2000, Windows Me y Windows XP emplean una base de datos central jerárquica, conocida como "Registro", para administrar software, configuración de dispositivos y ajustes de usuario.
   Los permisos impropios o ajustes de seguridad pueden permitir un acceso remoto al registro. Es posible que los atacantes exploten esta característica para comprometer el sistema o armar la base para ajustar la asociación de archivos y el permiso para habilitar código agresivo.
   Todas las versiones de Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows Me y Windows XP son vulnerables a un acceso remoto al registro. Para evitar caer ante esta vulnerabilidad se recomienda restringir el acceso al registro del sistema y revisar el conjunto de permisos para claves criticas del registro. Los usuarios de Windows NT 4.0 deben también asegurarse que el *Service Pack 3* ha sido instalado antes de ajustar el registro. Se deben tomar las medidas necesarias para restringir el acceso desde la red al registro, limitar el acceso remoto autorizado al registro. Microsoft liberó en Internet el articulo Q153183 de su base de conocimiento en donde se detalla como restringir el acceso a un registro NT desde una computadora remota.

10. **Anfitrión Windows de Programas (Scripts)**. En la primavera de 2000, el programa (*script*) de Visual Basic conocido como "Love Bug" causo millones de dólares en daños. Este gusano, y otros que le siguieron, se aprovecharon del Anfitrión Windows de Programas (*Windows Scripting Host WSH*), el cual permite que cualquier archivo de texto con una extensión ***.vbs*** sea ejecutada como un programa de Visual Basic. Con el WSH habilitado, un gusano típico se propaga incluyendo un código de Visual Basic como contenido de otro archivo y se ejecuta cuando ese archivo es visualizado o en algunos casos previsualizado.
    Algunos administradores se ocupan de tener las aplicaciones de navegadores, clientes de correo y plataformas de productividad constantemente actualizadas y parchadas, pero esto no los protege de los riesgos de los programas (*script*). El Anfitrión de Windows WSH puede ser deshabilitado en la mayoría de los sistemas en un esfuerzo proactivo para prevenir que los gusanos se esparzan.
    En maquinas con Windows 95 y NT, WSH se puede instalar manualmente o con Internet Explorer 5 y superior. WSH por default es instalado en Windows 98, Me, 2000 y XP. Por lo que estos son los sistemas más susceptibles a ataques por esta vulnerabilidad. Para proteger el sistema contra esta vulnerabilidad se recomienda deshabilitar o remover WSH como se indica en el conjunto de instrucciones de Symantec y Sophos. También se recomienda mantener activo el software antivirus y sus definiciones de virus actualizadas, algunos de estos programas antivirus permiten el bloqueo de *scripts.*

SISTEMAS UNIX Y LINUX

La historia del sistema operativo UNIX se remonta a 1968 cuando Ken Thompson y sus colegas del Computer Research Group en los Laboratorios Bell estaban trabajando en el proyecto Multics. El sistema Multics no fue lanzado, pero Ken Thompson desarrolló un sistema operativo a partir de él. Esta fue la primera versión de UNIX. En 1983, Thompson y Dennis Ritchie rescribieron UNIX en Lenguaje C, mejorando la robustez y confiabilidad del sistema haciéndolo fácil de

soportar. UNIX fue gradualmente transportado a otras plataformas y la funcionalidad del sistema operativo fue incrementada. Un buen número de organizaciones y academias apoyaron a UNIX, dándole las habilidades de comunicación por las que es famoso.

El sistema operativo UNÍX es una colección de programas que incluye editores de texto, compiladores y otros programas de utilidad. La arquitectura del sistema operativo UNÍX se muestra en la figura 4.1. [27]

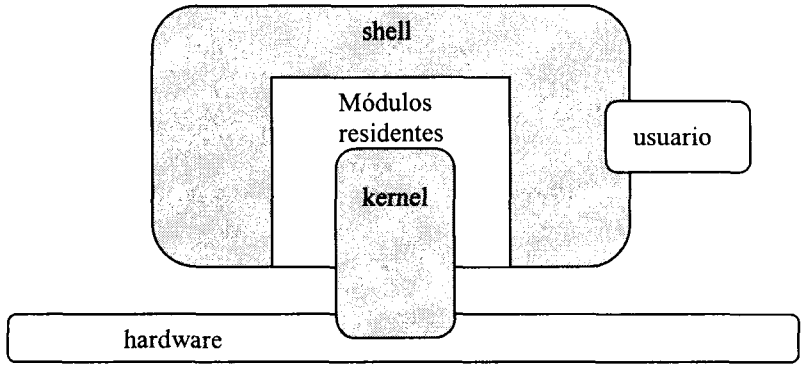


Figura 4.1 - Componentes del sistema UNIX

LINUX es un sistema de código abierto muy parecido al UNIX y que se ha vuelto muy popular hoy en día, dada esta similaridad, sus problemas de seguridad son tratados junto con los de UNIX.

A continuación se muestra las diez principales vulnerabilidades de seguridad que tienen el sistema UNIX y LINUX. [26]

1. **Llamadas de Procedimiento Remotas**. Las Llamadas a Procedimiento Remotas (RPCs) le permiten a los programas en una computadora ejecutar procedimientos en una segunda computadora enviando los datos y recuperando los resultados. RPC es ampliamente usado por muchos servicios distribuidos de red tales como administración remota, utilización compartida de archivos NFS, y NIS. Sin embargo hay múltiples fallas en RPC las cuales son activamente explotadas. En muchos casos, los servicios de RPC tienen privilegios de raíz al ejecutarse, y como consecuencia, los sistemas que ofrecen servicios RPC vulnerables le proveen al atacante un acceso remoto no autorizado a raíz del sistema. Se tiene evidencia que la mayor parte de los ataques del tipo "negación de servicio", realizados durante 1999 y principios del 2000, fueron ejecutados por sistemas victimas de las vulnerabilidades de las RPC. El ataque ampliamente exitoso en los sistemas de la milicia de los Estados Unidos durante el incidente Solar Sunrise también explotó una falla de RPC encontrada en cientos de sistemas del Departamento de Defensa de Estados Unidos.
   Los sistemas operativos afectados por estas fallas son casi todas las versiones de UNIX y LINUX ya que vienen con los servicios de RPC instalados y casi siempre habilitados. Para proteger el sistema de esta falla, se recomienda:
   - Apagar o remover cualquier servicio RPC que no sea absolutamente necesario para el funcionamiento de la red.
   - Instalar los últimos parches informáticos para cualquier servicio RPC que no se hayan podido remover. Para los sistemas LINUX se encuentran en http://www.debian.org./security.
   - Bloquear el puerto RPC (puerto 111) en el firewall que protege la red, y bloquear los puertos *loopback* 32770-32789 (TCP y UDP).

- Habilitar una pila no-ejecutable en los sistemas operativos que lo permita. Una pila no-ejecutable no protege contra el sobreflujo de buffer, pero hace más difícil la explotación de ataques de sobreflujo disponibles públicamente en Internet.

2. **Servidor Web Apache**. Muchos administradores de red consideran al servidor de web Apache completamente seguro si se compara con el Servidor de Información de Internet Microsoft. Esta comparación puede ser verdadera, aunque Apache no es invulnerable si se le pone bajo escrutinio. Las vulnerabilidades explotadas del núcleo Apache o de sus módulos han sido pocas, pero si han sido documentadas y utilizadas recientemente en ataques.
   Además, ningún servidor puede considerarse seguro si no se le ha probado hasta que es considerado en el contexto de su interacción con aplicaciones de red, especialmente programas de CGI y bases de datos. Una configuración reforzada de Apache puede dar acceso no autorizado a datos si los programas (*scripts*) CGI no son propiamente verificados o los controles de acceso a bases de datos no son ajustados correctamente. Los programas (*scripts*) CGI se ejecutan de igual manera que las instrucciones de servidor de web, de manera que un programa (*script*) malicioso o defectuosamente escrito es tan peligroso como una falla de software en Apache. Desgraciadamente estas fallas en la parte trasera del servidor permanecen como problemas hoy.
   También es imperativo fortalecer el sistema operativo para verdaderamente prevenir que contenido de web sea modificado o robado.
   Casi todos los sistemas LINUX y muchos otros sistemas UNIX traen Apache instalado y frecuentemente habilitado por default, así que todos estos sistemas tienen estas vulnerabilidades. Todos los sistemas UNIX son capaces de correr Apache. La versión de Apache para Windows probablemente tenga las mismas vulnerabilidades o similares. Se pueden tomar ciertos pasos para proteger el servidor Apache:
   - Obtener los últimos parches para Apache del sitio http://www.apache.org/dist/httpd/patches/. Y si es posible cambiar por la ultima versión del software.
   - Modificar el sistema de respuesta http de Apache. Esto permitirá al servidor retornar información falsa en su encabezado de respuesta, lo cual ayuda a esconder el software del servidor de Internet. Esto no evitara a un atacante determinado, pero puede proteger enormemente el servidor contra gusanos que accionan su código de ataque basados en la información regresada por el encabezado.
   - Se recomienda solo compilar en los módulos de Apache que el servidor requiera para funcionar apropiadamente. Al igual que con cualquier sistema que corre servicios innecesarios, Apache debe ser minimizado para reducir su exposición a problemas de seguridad.
   - Hay que considerar la opción de correr Apache en un ambiente *chroot()*. Para evitar que peticiones http maliciosas sean ejecutadas de manera exitosa, el servidor debe configurarse para inicializar con la función UNIX *chroot()*. Cuando un servidor de Internet inicia con esta función, el servidor de Internet no puede acceder ninguna parte de la estructura del directorio del SO fuera del área *chroot()* designada. Sin embargo cada servidor implementa *chroot()* de manera diferente y la documentación debe ser consultada.
   - No se debe correr Apache desde el directorio raíz. Se debe crear un nuevo usuario con privilegios mínimos en la red y en la base de datos ofrecidas por los servicios de Internet y ejecutar Apache como ese usuario.
   - Remover el contenido html por default, incluyendo los dos scripts CGI *test-cgi* y *printenv*. Las debilidades en el contenido por default son bien conocidas y frecuentemente atacadas.
   - Y lo más importante es asegurarse que el sistema operativo sobre el que se basa y los servicios que se ejecutan deben ser fortificados.

3. **Shell Seguro (SSH)**. Shell seguro (SSH) es un servicio popular para el aseguramiento de acceso de usuarios, ejecución de comandos, y transferencias de archivos en una red. La mayor parte de los sistemas UNIX utilizan el paquete *OpenSSH* o la versión comercial de *SSH Communication Security*. Aun y cuando SSH es mucho más seguro que Telnet, ftp, y programas de R-comandos, ha habido múltiples fallas en ambas implementaciones. La mayor parte son pequeños bugs, pero otros son problemas serios de seguridad que deberían ser reparados inmediatamente. El más peligroso de estos hoyos en la seguridad permite a los atacantes obtener acceso a raíz en una máquina desde una locación remota.
   El protocolo SSH1 ya ha demostrado ser potencialmente vulnerable a que una sesión sea desencriptada en transito dadas ciertas configuraciones. Por esta razón, se le recomienda a los administradores usar un protocolo más fuerte como el SSH2 siempre que sea posible. Además, los usuarios de OpenSSH deben notar que las librerías OpenSSL contra las que OpenSSH es típicamente construida tienen sus propias vulnerabilidades de software.
   Cualquier sistema UNIX o LINUX que corra OpenSSH 3.3 o anterior, o cualquier sistema UNIX o LINUX que corra SSH Communication Security SSH 3.0.0 o anterior son afectados por estas vulnerabilidades. Se recomienda para proteger este sistema:
   - Instalar la nueva versión de OpenSSH o SSH. En caso de que el sistema ya traiga las nuevas versiones buscar en el sitio de Internet los parches informáticos. En el caso de usar OpenSSL, asegurarse de utilizar las librerías más nuevas.
   - En la medida de lo posible, evitar usar el protocolo SSH1, ya que tiene debilidades de seguridad que ya fueron corregidas en la versión SSH2.
   - Implementar SSH incluye una variedad de opciones de configuración para restringir lo que las maquinas puedan conectar, y lo que los usuarios pueden autenticar, y determinar con que mecanismos pueden hacer eso. Los administradores deben determinar como estas opciones deben ser usadas en su ambiente en particular.

4. **Protocolo de Administración Simple de Red (SMNP)**. El protocolo de administración simple de red es usado extensamente para monitorear de manera remota y configurar casi todos los tipos de dispositivos modernos habilitados para TCP/IP. SNMP es frecuentemente usado para configurar y administrar dispositivos tales como impresoras, ruteadores, conmutadores, y para proveer la señal de entrada para servicios de monitoreo de red. La comunicación por medio de Administración Simple de Red consiste de distintos tipos de mensajes intercambiados entre las estaciones de administración SNMP y dispositivos de red, los cuales corren lo que es comúnmente conocido como software agente. El método por el cual estos mensajes son manejados, y el mecanismo de autenticación detrás del manejo de los mensajes tienen vulnerabilidades que son explotables.
   Existen un conjunto de vulnerabilidades en la forma en que mensajes trampa y mensajes de petición son manejados y decodificados por estaciones de administración y agentes. Estas vulnerabilidades no están restringidas a alguna implementación especifica de SNMP, sino que afectan distribuciones SNMP de vendedores. El resultado de atacantes explotando estas vulnerabilidades pueden ir desde la "negación de servicio" hasta configuración no deseada y administración de la maquinaria habilitada para SNMP.
   El mecanismo inherente de autenticación de las versiones anteriores SNMP también posee una vulnerabilidad significativa. Las versiones 1 y 2 de SNMP usan una "cadena comunitaria" no encriptada como único mecanismo de autenticación. La falta de encripción ya es suficientemente mala, pero la cadena comunitaria por default utilizada por la gran mayoría de los dispositivos SNMP es "pública", con unos pocos vendedores supuestamente listos que cambian la cadena a "privada" para información más sensible. Los atacantes pueden usar esta vulnerabilidad en SNMP para reconfigurar o apagar dispositivos de manera remota. El trafico SNMP analizado con sniffer puede revelar muchas cosas acerca de la estructura de la red, y de los sistemas y dispositivos

conectados a ella. Los intrusos usan tal información para escoger blancos y planear ataques.
La mayor parte de los vendedores activan la versión 1 de SNMP por default, y muchos no ofrecen productos capaces de usar los modelos seguros de la versión 3 de SNMP, que pueden ser configurados para usar métodos mejorados de autenticación. Sin embargo, hay reemplazos disponibles gratuitamente que proveen soporte para la versión 3 de SNMP bajo licencias GPL o BSD.
SNMP no es solamente para UNIX; es extensamente usado en Windows, en equipo de red, impresoras y otros dispositivos. Pero la mayoría de los ataques relacionados con SNMP que se han visto hasta ahora, ocurrieron en sistemas UNIX con pobres configuraciones de SNMP.
Casi todos los sistemas UNIX y LINUX vienen con SNMP instalado y frecuentemente habilitado por default, por lo que son afectados y están susceptibles a esta vulnerabilidad. La mayor parte de otros dispositivos habilitados SNMP y sistemas operativos también son vulnerables a ataques por esta causa. Las recomendaciones para proteger el sistema contra estas debilidades son:

- Si las SNMP no son necesarias hay que deshabilitarlas.
- Si es posible, emplear un modelo de seguridad SNMPv3 basado en el usuario, con autenticación de mensaje y encripción de la unidad de datos del protocolo.
- Si se tiene que usar SNMPv1 o v2, asegurarse que están corriendo las ultimas versiones con parches instalados.
- Filtrar SNMP (puerto 161 TCP/UDP y 162 TCP/UDP) en el punto de entrada de la red y no dejarlos entrar, a menos que sean absolutamente necesarios para administrar dispositivos externos.
- Emplear accesos de control basados en la terminal en los agentes de sistema SNMP. Mientras que esta capacidad puede estar limitada por las capacidades del agente SNMP del sistema operativo, es posible controlar de que sistemas el agente aceptara peticiones. En los sistemas UNIX esto puede lograrse por medio de un envoltorio TCP o configuración Xinetd.

5. **Protocolo de Transferencia de Archivos (FTP)**. El daemon FTP es usado para distribuir archivos a usuarios anónimos o autenticados por medio de un *nombre de usuario y password.* Los servicios anónimos de FTP no requieren un password única y todos los usuarios utilizan el mismo nombre de acceso ("anónimo" o "ftp"), permitiendo a todos acceder el servicio.
Los servicios autenticados de FTP si requieren un nombre de usuario y password, pero ambos son transmitidos sobre la red a manera de texto en claro (plain text), permitiendo que una tercera persona intercepte el intercambio de credenciales. Para robar la información de acceso FTP, un atacante necesita colocar un *sniffer* de red en algún lugar a lo largo de la trayectoria de conexión, tal como la LAN del servidor FTP o en la LAN cliente.
Además de esta inherente inseguridad de transmisión, fallas criticas han sido encontradas en muchas versiones del software para el servidor FTP, ya sean provistas por los vendedores de sistemas operativos (Sun,HP-UX,etc) y aquellas desarrolladas por la comunidad de código abierto (WU-FTPD, ProFTPD, etc). Muchas vulnerabilidades le permiten a un atacante obtener acceso a la máquina que es anfitrión del servidor FTP, mientras que otras solo permiten ejecución de comandos a un nivel usuario. Por ejemplo, las vulnerabilidades de WU-FTPD le permite a los atacantes ganar acceso a raíz y copiar sus herramientas tales como kits para raíz y entonces usar al sistema para propósitos oscuros. La mayoría de estas vulnerabilidades requieren que este habilitado el acceso anónimo, aunque algunas trabajan aun y cuando el acceso anónimo esta negado y así seguirá mientras el servidor FTP escuche al puerto de red. Debe notarse que, aunque el servidor FTP usa una llamada de sistema ***chroot()*** para confinar un usuario anónimo a un

directorio especificado, aun puede ser explotado debido a grandes fallas en la implementación.
Los sistemas operativos afectados por esta vulnerabilidad son casi todos los UNIX y LINUX, ya que estos vienen con al menos un servidor FTP instalado y habilitado. Hay varios pasos que aplicar para la protección del sistema:

- Instalar la nueva versión de FTP que se use. Los servidores FTP más populares y gratuitos son WU-FTPD y Pro-FTPD.
- Deshabilitar los accesos anónimos a servicios FTP si no son necesarios. Para hacer esto en las distintas versiones de UNIX y LINUX se deben seguir las instrucciones en sus manuales. Para WU-FTPD y Pro-FTPD, hay que crear o editar el archivo */etc/ftpusers* y agregar los nombres de usuario "anónimo" y "ftp" en él. En el archivo se detalla que usuarios no deben ser permitidos en accesar al servidor FTP. Para agregar una capa adicional de seguridad, remover el usuario "ftp" del archivo de password.
- En caso de que la funcionalidad anónima sea necesitada, asegurarse que la funcionalidad de subir archivos anónimamente este deshabilitada, para que los usuarios necesiten un nombre de usuario valido y un password para poner archivos en el servidor. Estas características generalmente están deshabilitadas.
- Restringir el acceso al servidor FTP por la dirección de IP o de dominio utilizando envoltorios TCP. Los envoltorios TCP son instalados por default en las versiones mas recientes de UNIX y LINUX. Si se escribe una línea similar a "*in.ftpd: 10.164.168.15*" o "*in.ftpd: .good_domain.com*" en el archivo */etc/hosts.allow*, así solo se le permitirá el acceso desde direcciones IP especificas. Para complementar, se debe colocar "*in.ftpd: ALL*" en */etc/hosts.deny* para bloquear el acceso desde las otras direcciones, y confirmar que el daemon FTP sea iniciado vía "tcpd" en */etc/inetd.conf.*
- Implementar permisos restrictivos de archivos en el servidor FTP para que los usuarios sean capaces de accesar solo los archivos necesarios.
- Deshabilitar los servidores FTP no usados completamente y remover el software del sistema. Los firewalls bloquearán el puerto 21 en el perímetro de dispositivos si FTP no es utilizado por razones de negocios.

6. **Servicios Remotos, Confianza en relaciones**. A Shell remoto (rsh), copiado remoto (rcp), acceso remoto(rlogin), y ejecución remota (rexec) se les conoce de la manera colectiva como "comandos-R", y son ampliamente utilizados en el mundo UNIX. Organizaciones con múltiples servidores UNIX frecuentemente configuraran los "Servicios-R" correspondientes (in.rshd, in.rlogind, in.rexecd) de tal manera que los usuarios se pueden mover de una máquina a otra sin tener que escribir un clave de usuario y password cada vez que se muevan. Incluso en redes donde los recursos de un usuario dado están contenidos en un solo sistema, los administradores son casi siempre responsables por docenas o cientos de sistemas, por lo que configuran los servicios remotos para facilitar su propio movimiento de máquina a máquina. Un solo usuario puede ejecutar RSH, RCP, RLOGIN o REXEC desde una máquina A hacia una máquina B sin tener que hacer una nueva autenticación colocando el nombre o dirección de la máquina A en el archivo ***~/.rhosts*** de la máquina B. Todos los usuarios pueden ejecutar RSH, RCP, RLOGIN o REXEC desde la máquina A hacia la máquina B sin tener que volver a autenticarse sí el nombre o la dirección de la máquina A esta en el archivo ***/etc/hosts.equiv*** de la máquina B.
Los servicios remotos sufren las dos fallas fundamentales en las conexiones de red: la falta de encripción y una pobre autenticación de anfitrión (host). La transmisión de información, en forma de texto en claro, entre clientes de comandos remotos y los servicios remotos permite que los datos o presiones de teclas sean interceptadas. El hecho de que los servicios remotos simplemente acepten el nombre o la dirección presentados por un cliente que se conecta permite que se haga una fabricación falsa de información. Sin relaciones de

confianza establecidas, los usuarios son forzados a enviar passwords sobre la red de manera desprotegida. Con relaciones de confianza (*trust*), un atacante puede asumir la identidad de un usuario valido en un anfitrión valido, y usarlo para obtener acceso a todas las otras máquinas que confían en la máquina pirata.
Casi todas las versiones de UNIX y LINUX traen los servicios remotos instalados y habilitados, por lo que son susceptibles a explotación de esta vulnerabilidad. Para proteger el sistema de esta vulnerabilidad se deben deshabilitar los servicios remotos en cualquier sistema donde no sean absolutamente necesarios. *Secure shell* y sus complementos *scp* y *sftp* pueden reemplazar de manera más segura la funcionalidad de todos los servicios remotos. Si los servicios remotos son absolutamente necesarios, deshabilitar las relaciones de confianza (*trust*) y utilizar los envoltorios TCP para grabar todos los intentos de conexión, restringir el acceso a anfitriones específicos, y proveer de verificación del anfitrión. Para deshabilitar las relaciones de confianza, remover el archivo */etc/hosts.equiv* y el archivo *~/.rhosts* de cualquier usuario. Si se deben usar relaciones de confianza, nunca utilizar el carácter comodín "+", ya que puede ser usado para permitir cualquier usuario o maquina para accesar con credenciales validas, asegurarse de usar los envolventes TCP. Nunca usar *~/.rhosts* para permitir autenticación de raíz sin password.

7. **Daemon de Impresora de Línea**. El daemon Berkeley de impresora de línea (LPD) es históricamente el servicio que deja a los usuarios conectarse a una impresora local desde una máquina local o desde una máquina remota en el puerto TCP 515. Aun y cuando hay servidores de reemplazo disponibles, LPD persiste como el servidor de impresión más comúnmente usado en las distribuciones de UNIX y LINUX. Muchas implementaciones de LPD, contienen fallas de programación que han llevado a desbordamientos de flujo permitiendo a atacantes correr código arbitrario con privilegios de raíz. Muchas versiones distintas de sistemas UNIX contienen daemons LPD vulnerables.
Casi todos los sistemas UNIX y muchos de LINUX vienen con una versión instalada de LPD y habilitada por default, con lo que son susceptibles a explotación de esta vulnerabilidad. Con el fin de evitar que esta vulnerabilidad cause estragos en el sistema, se recomienda revisar el CERT Advisory 2001-30 para la información especifica del sistema operativo. Si la terminal no tiene porque actuar como un servidor de impresión para peticiones remotas, se puede deshabilitar el servicio "*in.lpd*" en los archivos *inetd o xinetd*. Para inetd, borrar la línea "in.lpd" en el archivo /etc/inetd.conf o en /etc/inet/inetd.conf y reiniciar inetd. Para xinetd, agregar "disable=yes" al archivo "in.lpd" y reiniciar xinetd. Si se necesita dar servicio a las peticiones de servicios de impresión remotos, restringe lo que los anfitriones puedan conectar en in.lpd con los envoltorios TCP.
Se puede proveer algo de protección contra los sobreflujos de buffer al habilitar una pila no ejecutable en los sistemas operativos que soporten esta opción. Esto evitara contra los ataques públicamente disponibles en Internet aunque no protegerá contra todos los sobreflujos de buffer.

8. **Envío de correo (sendmail)**. Sendmail es el programa que envía, recibe, manda adelante la mayor parte del correo electrónico procesado en computadoras UNIX y LINUX. El extenso uso de sendmail en Internet lo ha hecho un blanco principal de ataques, lo que resulta en numerosos agujeros a explotar con el paso del tiempo.
La mayor parte de estos ataques son exitosos solo contra las versiones más viejas del software. A pesar del hecho que estos viejos problemas están bien documentados y han sido reparados en nuevas versiones, aun existen muchas versiones viejas o mal configuradas que se siguen usando, por lo que sendmail sigue siendo uno de los servicios mas frecuentemente atacados.
Los riesgos de utilizar sendmail pueden agruparse en dos categorías: Escalamiento de privilegios causados por desbordamiento de buffer, y una impropia configuración que permite a tu máquina ser un punto de redirección para el correo electrónico desde cualquier

otra máquina. Este último es un problema en cualquier sistema que corre versiones más viejas del código. Esto resulta de usar ya sea configuración default de archivos o impropia, y es uno de los principales obstáculos para evitar la proliferación del correo basura (*spam*).
Casi todos los sistemas UNIX y LINUX vienen con una versión de sendmail instalada y habilitada por default, haciéndolos vulnerables. Para proteger sendmail se pueden descargar los parches más nuevos o instalar una versión mas actualizada de sendmail, otra opción es evitar ejecutar sendmail en modo daemon en maquinas donde esta habilitado por default este servicio, en caso de que se necesite correr sendmail en modo daemon hay que asegurarse que la configuración esta diseñada para redirigir el correo apropiadamente y solo en sistemas que estén bajo la supervisión del administrador, se puede explorar el sitio http://www.sendmail.org/tips/relaying.html para tener asistencia al configurar propiamente el servidor. Debe uno asegurarse que sendmail no este siendo usado para redireccionamiento. Cuando se actualice la versión de sendmail se debe asegurar que el archivo de configuración sea también actualizado, ya que las configuraciones viejas pueden permitir el redireccionamiento aun y cuando se corra nuevo código.

9. **BIND/DNS**. El paquete Nombre de Dominio de Internet Berkeley (BIND) es la implementación más usada de Sistema de Nombres de Dominio (DNS), BIND ha sido frecuentemente blanco de ataques. Los desarrolladores de BIND han corregido rápidamente las vulnerabilidades, aunque aun siguen en uso un buen número de servidores viejos y mal configurados.
   Varios factores contribuyen a esto, principalmente los administradores que no se dan cuenta de la existencia de actualizaciones de seguridad, de sistemas que utilicen el daemon BIND innecesariamente, y de mala configuración de archivos. Cualquiera de estos puede causar "negación de servicio", desbordamiento de archivos o envenenamiento de caché de DNS. En un ejemplo de "negación de servicio" un atacante puede enviar paquetes DNS específicos para forzar un chequeo interno de consistencia, el cual es vulnerable y causara que el daemon BIND se apague. Un ejemplo de un ataque de desbordamiento de flujo, un atacante utiliza implementaciones vulnerables de las librerías del resolutor DNS. Al enviar respuestas DNS maliciosas, el atacante puede explorar esta vulnerabilidad y ejecutar código arbitrario o incluso causar una "negación de servicio".
   Además del riesgo que presenta un BIND vulnerable para el servidor que lo contiene, una sola máquina de seguridad rota puede ser una plataforma para actividad maliciosa que apunta a otras máquinas en Internet, o que sean usadas como deposito de material ilícito sin el conocimiento del administrador.
   Casi todos los sistemas UNIX y LINUX vienen con una versión de BIND instalada y habilitada por default, con lo que están expuestos a esta vulnerabilidad. La protección en esta situación puede llevarse a cabo al emplear las siguientes recomendaciones:
   - Deshabilitar el daemon BIND en cualquier sistema que no este específicamente diseñado y autorizado para ser un servidor DNS.
   - Aplicar los parches o actualizar el sistema del servidor DNS a su ultima versión.
   - Para hacer más difíciles los ataques automáticos al sistema, ocultar la bandera "versión String" en BIND reemplazando la versión actual de BIND con un número de versión falso en la línea del archivo de opciones "*named.conf*".
   - Permitir transferencias de zona solo a servidores DNS secundarios en tu dominio. Deshabilitar transferencias de zona a dominios padre o hijo, utilizando en lugar de las transferencias delegación y envío hacia adelante.

10. **Autenticación en general en UNIX y LINUX**. Las palabras de pase, frases de pase y códigos de seguridad son usadas en casi cualquier interacción entre usuarios y sistemas de información. La mayor parte de autenticación de usuarios, al igual que la protección de datos y archivos, se basan en passwords dadas por usuarios. Un password comprometido da la oportunidad de explorar un sistema desde su interior sin ser detectado, ya que si se

entra de manera legal y autenticada no es probable que se levanten sospechas. Así, un atacante tendrá acceso completo a los recursos disponibles para este usuario, y estará significativamente cerca de poder accesar otras cuentas, máquinas cercanas, y quizás hasta privilegios administrativos. A pesar de estos riesgos, las cuentas con malas o vacías passwords siguen siendo muy comunes, y las organizaciones con buenas políticas de passwords no son comunes.

Las vulnerabilidades de password más comunes son:

a) Cuentas de usuario que tienen passwords débiles o que simplemente no tienen una.
b) A pesar de la fortaleza de su password, los usuarios fallan en mantenerla secreta.
c) El sistema operativo o el software adicional crea cuentas administrativas con paswords débiles o sin ellas.
d) Algoritmos *hash* para password son conocidos y frecuentemente los valores *hash* son almacenados de manera que son visibles por cualquiera.

La mejor defensa contra esto es tener una fuerte política de password la cual incluya instrucciones completas para buenos hábitos con passwords y una revisión proactiva de su integridad.

Todos los sistemas operativos o aplicaciones en donde los usuarios usen autenticación por medio de un ID y password son débiles ante esta vulnerabilidad. Para defender el sistema contra esta amenaza se puede aplicar una política fuerte la cual incluya instrucciones precisas con la finalidad de engendrar buenos hábitos de passwords y una revisión proactivo de la integridad de passwords. El encargado de la seguridad se debe asegurar que los passwords sean resistentes, ya que con suficientes recursos de hardware y tiempo cualquier password puede ser descubierta por métodos de fuerza bruta. Las recomendaciones en cuanto a la creación de password serán vistas con mas detalle en las configuraciones de sistemas. Una vez que los usuarios han sido instruidos en la creación de passwords resistentes, deben asegurarse de utilizar los procedimientos para seguir las instrucciones de passwords. Una buena manera de hacerlo es validar el password siempre que el usuario lo cambie, muchas de las versiones de UNIX pueden usar ***Npasswd*** para revisar las passwords introducidas y compararlas con las políticas. Es importante verificar la resistencia de los passwords continuamente y tratar de aplicar revisiones contra diccionarios, si esto no es posible entonces hay que correr utilerías de descifradoras (*cracking*) con los permisos correspondientes de los dueños de la empresa. Si los problemas con el uso de passwords son muchos entonces se puede optar por utilizar medidas biométricas de autenticación, tal y como se verá en la sección de ***controles físicos*** de las configuraciones de sistemas. Se deben proteger los passwords aunque se hayan escogido para ser resistentes, si se guardan los valores *hash* de passwords en el archivo */etc/passwd*, hay que actualizar el sistema para usar el archivo */etc/shadow.* Si el sistema corre NIS o LDAP y los valores hash no pueden protegerse, cualquiera puede leer los valores hash de los passwords e intentar descifrarlos. Por tanto, se debe asegurar tener los permisos propios. También se debe mantener una lista maestra de las cuentas de usuarios con la cual hacer auditorias de seguridad, sin olvidar los passwords para los ruteadores, impresoras conectadas a Internet, copiadoras y controladores de impresoras, y tener la capacidad de borrar las cuentas cuando ya no estén en uso y de incluir nuevas cuentas autorizadas. El administrador de seguridad debe diseñar procedimientos rigurosos para remover las cuentas cuando los empleados o los contratistas sean despedidos y que sus cuentas no sean necesarias. Existen herramientas disponibles para ayudar con una buena política de passwords, por ejemplo ***Symantec Enterprise Security Manager*** (ESM) permite el monitoreo de cualquier cambio en políticas, creación de nuevas cuentas y resistencia de passwords. ESM intentara descifrar passwords mientras desempeña la ejecución de políticas en la red. ESM monitorea los registros de accesos y cualquier cambio que haya sido hecho a la estructura de la red.

SISTEMA SOLARIS

El ambiente operativo SOLARIS es un sistema operativo flexible y de propósito general. Solaris de la compañía Sun Microsystems es ampliamente utilizado hoy en día, y por tanto también ha sufrido numerosos ataques a su seguridad. Los ataques se basan en la explotación de vulnerabilidades.

A continuación presentaremos las principales vulnerabilidades que afectan al sistema Solaris: [28]

1. Una vulnerabilidad que es causada por un usuario es la de conectar el sistema Solaris a alguna red pública antes de instalar los parches de seguridad o configurarlos para un modo más protegido. Al hacer esto, se les presenta a posibles atacantes una gran oportunidad para crear puertas traseras ya que el sistema aun tiene presentes sus vulnerabilidades. El instalar actualizaciones también requiere cuidado, ya que muchas de las configuraciones regresan a su estado original y el sistema queda de nuevo expuesto a incursiones de atacantes. Por ello, se recomienda no conectar el equipo o red que maneje Solaris a una red pública antes que las modificaciones de seguridad sean completadas, se debe tener cuidado de examinar todos los archivos *init* de scripts y probar los cambios que causa cada parche de actualización en máquinas fuera de la red.

2. El hardware SPARC de Sun provee de características adicionales de seguridad. Esto evita cambios en la EEPROM, ejecución de comandos de hardware, e inicios de sistema sin el password adecuado. Esta protección de password solo funciona mientras que el sistema esta en el nivel *OpenBoot PROM.* Cuando se habilita el modo de seguridad ***command*** o ***full*** de EEPROM, la perdida del password de *PROM OpenBoot* puede requerir que se cambie la EEPROM. La debilidad aquí esta en que si hay un atacante con privilegios de súper usuario este puede cambiar el modo de seguridad a ***full***, colocar caracteres aleatorios en el password y reiniciar el sistema. El sistema ya no reiniciara sin el password nuevo, y por tanto el sistema ya no podrá ser usado. En este caso hay que contactar a la organización SunService para arreglar el problema.

3. Los bits de ***set-user-ID*** y ***set-group-ID*** (a veces llamados bits de SUID y de SGID) en un archivo ejecutable le indican al sistema que el archivo ejecutable debe operar con los privilegios del usuario dueño o del grupo dueño del archivo. Un archivo de ***set-group-ID*** modifica la ID efectiva de grupo del programa corriendo por la del grupo del archivo ejecutable. Este archivo es útil para permitirle a los usuarios correr algunos comandos que reúnen información del sistema o el escribir en archivos que no son del usuario. Los comandos de ***set-user-ID*** y ***set-group-ID*** que tienen fallas son frecuentemente usados para explotar el sistema. El atacante usa los privilegios elevados provistos por el mecanismo ***set-user-ID*** o ***set-group-ID*** para ejecutar código en la pila del programa (un ataque del tipo "sobreflujo del buffer") o para sobrescribir archivos del sistema. Los atacantes pueden usar las características de ***set-user-ID*** o ***set-group-ID*** para crear puertas traseras (*backdoors*) en los sistemas. Una manera de hacer esto es copiando el *shell* del sistema a una locación "escondida" y agregarle el bit de ***set-user-ID***. Esta técnica le permite al atacante ejecutar el *shell* para ganar privilegios elevados. Para enfrentar este problema, si se reporta esta vulnerabilidad a Sun Microsystems, la compañía los arregla y provee parches informáticos. Esta es otra razón por la que se debe mantener el sistema con los últimos y más nuevos parches.

4. Los atacantes a veces usan los archivos ***set-user-ID*** para obtener privilegios elevados. Estas puertas traseras pueden esconderse en cualquier lugar del sistema. Para proteger el sistema, se debe saber que, aunque un archivo pueda tener un bit de ***set-user-ID***, esto no es efectivo en sistemas de archivos montados con la opción ***nosuid***. Así, el sistema

ignorará el bit de ***set-user-ID*** para todos los archivos en un sistema de archivos montado con ***nosuid***, y los programas se ejecutan con privilegios normales. Es posible montar un sistema de archivos en el modo de solo-lectura para prevenir modificaciones de archivos. Esta configuración previene que un atacante guarde archivos de puertas traseras o sobrescribir y reemplazar archivos en un sistema. Siempre que sea posible, los sistemas de archivos deben ser montados en modo de solo-lectura, y configurados para ignorar el bit ***set-user-ID*** en los archivos. Sin embargo, hay que recordar que un sistema de archivos de solo lectura puede ser remontado en modo lectura-escritura. La opción ***nosuid*** puede ser removida. No todos los sistemas Solaris pueden ser montados en el modo solo-lectura o con ***nosuid***. Si un sistema de archivos es remontado en modo lectura-escritura, debe ser reiniciado para cambiarlo a solo-lectura. también se requiere reiniciar el sistema de ***nosuid*** a ***suid***. Hay que tener especial cuidado con los reinicios de sistema no programados.

5. Si la administración de volúmenes es necesaria, las opciones de montado para algunos sistemas de archivos pueden ser modificadas por seguridad. En versiones de Solaris previas a la versión 8, la configuración por default del Solaris Volume Manager es permitir sistemas de archivos ***suid*** para todos los medios removibles capaces de soportarlo. En la versión 7 de Solaris y en versiones anteriores, cualquiera podía insertar un disco formateado UFS que contiene un ***set-user-ID*** ejecutable y así ganar control del sistema. Para evitar esta situación, se recomienda agregar las siguientes líneas al final del archivo */etc/rmmount.conf* en todas las versiones previas a la 8 de Solaris OE:

   Mount hsfs –o nosuid
   Mount ufs –o nosuid

   Las versiones después de la 8 ya tienen estas líneas en el archivo por default. Con estas opciones, el bit ***set-user-ID*** en archivos ejecutables es ignorado en sistemas de archivos que son montados por el sistema Solaris Volume Manager. Otro problema de seguridad existe cuando usa medios de escritura automontados, como los discos, discos zip, etc. Estos tipos de medios son montados automáticamente como públicamente legibles y escribibles. Estos tipos de medios representan un riesgo de seguridad en sistemas multiusuario ya que cualquier usuario en el sistema puede leer, escribir, y modificar los contenidos de los medios automontados. Se recomienda poner cuidado en asegurarse que usuarios no autorizados sean incapaces de acceder o modificar información sensible a través de los medios escribibles automontados.

6. Los sistemas ***at, cron*** y ***batch*** ejecutan comandos en un tiempo especifico en el futuro. Las peticiones de usuarios para el sistema cron son manejadas por el comando ***crontab.*** Los comandos ***at*** y ***batch*** son utilizados para enviar tareas al sistema ***at.*** Los sistemas ***cron*** y ***at*** pueden ser problemáticos porque ejecutan comandos en el futuro. Un atacante puede usar estos sistemas para implementar una "bomba lógica" u otro tipo de ataque programado que comience en algún punto del futuro. Si no se examina cada petición de ***at, batch*** y ***cron***, el rastreo del uso y abuso de sistemas puede ser difícil. Se recomienda que el acceso a los sistemas ***at, batch*** y ***cron*** este restringido para prevenir ataques y abusos. Por default, el ambiente Solaris incluye eventos ***cron*** calendarizados para las cuentas ***lp, adm,*** y ***root***. Estas calendarizaciones no deberían ser incluidas en los archivos de negación de acceso. Cualquier sistema adicional o cuentas especificas de software que no requieren acceso ***cron, at*** o ***batch*** deben ser incluidos en el listado de archivos con acceso negado. Para tener un control sobre las cuentas de usuario que necesitan acceso hay que crear un archivo de permisos (*allow file*) y agregar ahí las cuentas de usuarios necesarias.

7. En versiones previas a 8 del ambiente Solaris, la mascara de creación de modo de sistema de archivos para el ambiente Solaris es 000. Este default significa que los archivos creados

por los daemons del sistema, son creados con bits de permiso que son 666 (legibles y modificables por todo usuario). Este default puede ser un problema, porque les da a los usuarios normales permiso para sobrescribir los contenidos de los archivos del sistema. La versión 8 del ambiente Solaris fue la primera en la que ***umask*** default es cambiada a 022. Las versiones mas nuevas tienen aun más cambios. El valor default de 022 es definido por la variable ***cmask*** en el archivo ***/etc/default/init*** y puede ser modificada al cambiar el valor ***cmask.*** Para las versiones anteriores a la 8 de Solaris, debe usarse el siguiente script para colocar ***umask*** en un valor más razonable:

```
echo "umask 022" > /etc/init.d/umask.sh
chmod 744 /etc/init.d/umask.sh
chgrp sys /etc/init.d/umask.sh
for d in /etc/rc ?.d; do
        Ln /etc/init.d/umask.sh $d/SO0umask.sh
done
```

8. Algunos programas encargados de explotar vulnerabilidades de seguridad toman ventaja del kernel de pila de sistema ejecutable del Solaris para atacar al sistema. Estos programas de ataques intentan sobrescribir partes de la pila de un programa privilegiado en un intento de controlarlo. Para proteger el sistema de esta vulnerabilidad se recomienda. En la versión 2.6 de Solaris y posteriores, estas vulnerabilidades pueden ser evadidas haciendo la pila del sistema no-ejecutable. Para ello se pueden agregar las siguientes líneas al archivo */etc/system:*

   ```
   set noexec_user_stack = 1
   set noexec_user_stack_log = 1
   ```

   Con ***noexec_user_stack_log*** habilitado, el sistema almacena los intentos programaticos de ejecutar código en la pila. Esta característica permite rastrear los poco exitosos intentos de los programas y la cuenta que los hizo. Con estas líneas la pila se hace no-ejecutable, lo cual provee cierta protección contra vulnerabilidades para las que no se ha liberado parche alguno. Sin embargo, esto no protege contra los programas que utilizan otros principios, por lo que se vuelve a recomendar la instalación de los últimos parches de seguridad. La característica de hacer la pila no ejecutable solo funciona con las siguientes arquitecturas SPARC: hardware sun4d, sun4m, y sun4u.

9. Los archivos del núcleo contienen la imagen de memoria de un proceso en ejecución que fue terminado al recibir cierta señal. Estos archivos son frecuentemente usados para investigar errores de programa. Hay dos problemas con ellos: consumen espacio y contienen información sensible. Un archivo de núcleo puede contener información privilegiada que los usuarios no deberían poder acceder. Mientras esta corriendo, el proceso puede leer al archivo ***/etc/shadow*** para revisar un password o cargar un archivo de configuración protegido. Estas son piezas de información que normalmente están escondidas para los usuarios pero que pueden existir en el archivo del núcleo. Esta información puede ser usada para atacar al sistema. Por razones de seguridad, el ambiente Solaris no escribe archivos de núcleo con un ID efectivo que sea diferente del ID real. Esta restricción significa que ***set-user-ID*** y los programas ***set-user-ID*** no crean archivos de núcleo. Si los archivos de núcleo deben ser usados para *debugging* de aplicaciones, hay que borrar los archivos viejos. De vez en cuando, hay que buscar en el sistema viejos archivos de núcleo y borrarlos. Esta practica también ayuda a que el sistema no se llene de archivos viejos. A partir de la versión 7 del sistema Solaris se incluyó una utilería para administrar archivos de núcleo, el comando ***coreadm*** permite que un administrador defina los nombres de archivos y directorios para los archivos de núcleo.

10. Los servicios de red del sistema Solaris pueden ser atacados de muchas maneras. Estos servicios pueden contener fallas de programación, usar ninguna o débil autenticación, transferir información sensible en formato no encriptado y permitir conexiones desde cualquier anfitrión (*host*). Estas debilidades permiten que un sistema sea comprometido fácilmente por un atacante. Hay varios métodos para reducir el riesgo de ataques exitosos, los administradores deben deshabilitar los servicios no necesarios y aplicar todos los parches de seguridad disponibles y utilizar servicios de seguridad. Solaris 9 OE es la primer versión en incluir varias herramientas que pueden proveer protección a los servicios de red: Solaris Secure Shell, Kerberos Key Distribution Cente, Envolventes de TCP. Para las versiones 8 y anteriores de Solaris existen SunScreen y SunScreen Lite, los cuales son productos de Sun Microsystem que proveen protección a la red, ambos se comportan como firewalls y proveen control de accesos en red. SunScreen Lite es una versión gratis del SunScreen y esta limitado a usar dos interfases de red, y aun así provee protección adecuada para los servicios de red. En Solaris 9 OE se incluye la versión completa de SunScreen 3.2 de manera gratuita. OpenSSH y SSH son plataformas de herramientas que reemplazan los comandos inseguros de redes UNIX tales como ***telnet, ftp, rlogin, rsh*** y ***rcp*** y proveen de un túnel seguro para comunicación en redes. OpenSSH y Solaris Secure Shell proveen fuerte autenticación y privacía a través de encripción. Cuando OpenSSH se construye con la librería de Envolvente de TCP, OpenSSH se beneficia de su control de accesos, el cual es usado con Solaris Secure Shell. Los programas Envolventes de TCP proveen de control de accesos a nivel TCP y verificación del nombre de anfitrión DNS. Los Envolventes de TCP pueden ser usados para proteger servicios de red manejados por ***inetd***; esta herramienta provee un mejor mecanismo de acceso y detecta discrepancias de nombres DNS que pueden indicar que un ataque esta en progreso.

CONFIGURACIONES DE SISTEMAS COMPUTACIONALES y RECOMENDACIONES DE SEGURIDAD

JUSTIFICACIÓN

En esta sección se presentan distintas configuraciones de sistemas de computo y recomendaciones de seguridad por medio de la utilización de herramientas y técnicas de seguridad. Las configuraciones son las que podemos encontrar con mayor facilidad en alguna empresa o negocio. No se pretende mencionar todas las configuraciones existentes sistemas de computo, solo las más usuales, por lo que la finalidad es que este documento sea de utilidad para todo aquel que desee iniciarse en la seguridad informática y sirva de base en las decisiones al escoger las técnicas o herramientas más apropiadas para la configuración que le corresponda; mostrando la forma en que la aplicación de las herramientas y técnicas afectan al sistema y su desempeño. Para las configuraciones de sistemas informáticos las recomendaciones se dividen en las secciones correspondientes a los mecanismos de defensa mencionados en la página 20, es decir, se hacen en las áreas de Encripción, Controles de Software, Controles de Software, Controles Físicos y Políticas. Si se siguen de manera adecuada las recomendaciones que se hacen, se puede lograr de manera efectiva realizar operaciones y transacciones a través de una red o Internet. Las recomendaciones también cubren el caso en que solo se busca proteger la

información interna del sistema y se carece de una conexión a Internet o a alguna red, resguardando la información que contiene la computadora para que no haya usuarios malintencionados que ganen acceso a ella, aprovechando las vulnerabilidades propias de cada sistema operativo y de los paquetes de software que se utilicen.

Para poder facilitar la comprensión del efecto que causa el aplicar cierta técnica o herramienta de seguridad recomendada, se incluye una calificación para la seguridad del sistema antes y después de aplicar las recomendaciones. En la tabla 4.1 se definen las características de cada nivel de seguridad.

Tabla 4.1 - Niveles de seguridad

1	Sistema protegido contra acceso de usuarios no autorizados y protegido contra virus informáticos conocidos.
2	Sistema protegido contra acceso de usuarios no autorizados, virus informáticos, protección de la integridad de la información manejada y transmitida, y establecimiento de políticas de seguridad.
3	Sistema protegido contra acceso de usuarios no autorizados, virus informáticos, protección de la integridad de la información manejada y transmitida, establecimiento de políticas de seguridad, protección contra las vulnerabilidades conocidas del sistema operativo y protección del hardware contra robo físico.
4	Sistema protegido contra acceso de usuarios no autorizados, virus informáticos, protección de la integridad de la información manejada y transmitida, establecimiento de políticas de seguridad, protección contra las vulnerabilidades conocidas del sistema operativo, protección del hardware contra robo físico y capacidad de detección de actividad inusual dentro del sistema.
5	Sistema protegido contra acceso de usuarios no autorizados, contra virus informáticos, protección de la integridad de la información manejada y transmitida, establecimiento de políticas de seguridad, protección contra las vulnerabilidades conocidas del sistema operativo, protección del hardware contra robo físico, capacidad de detección de actividad inusual dentro del sistema, control y análisis de tráfico que circula en la red, y protección del sistema computacional contra accesos piratas desde Internet.

La elección de las herramientas de seguridad requiere la consideración del costo en operatividad del sistema informático. Entre más aislado y mayores medidas de seguridad contenga el sistema, su utilidad y operatividad serán menores. Por ello, se puede interpretar que la operatividad es inversamente proporcional a la seguridad del sistema. Chiristian Fabian Borghello lo propone de una manera simple en su tesis.[25]

$$Operatividad = \frac{1}{Seguridad}$$

Así, basándonos en esta formula se otorgara también una calificación para la operatividad del sistema de acuerdo a su nivel de seguridad. La calificación será de **0.2** a **1**, siendo **0.2** la calificación mínima de operatividad, donde el sistema estará lleno de herramientas de seguridad, y **1** para la operatividad máxima donde los elementos de seguridad serán pocos.

CONFIGURACIÓN 1 - Una sola computadora sin conexión a Internet

Se pueden tener distintas configuraciones de sistemas en los que se hace necesaria la implementación de elementos de seguridad. En primer lugar se supondrá el caso de que se tiene solamente una estación de trabajo sin acceso a Internet o a alguna otra red de información. Las características por default de seguridad de una terminal de este tipo consisten en: un sistema operativo sin sus parches de seguridad instalados, ningun tipo de autenticación de usuario o encripción de archivos importantes y ningun software de auditorias. Muchos de los equipos de

computo vienen de fabrica con programas antivirus instalados (aunque no necesariamente actualizados) y candados o elementos de seguridad física. En suma, la seguridad de este equipo es pobre.

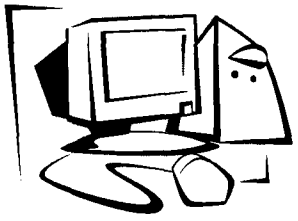


Figura 4.2 - Una sola computadora sin conexión a Internet

ENCRIPCIÓN

El uso de la encripción en este caso es poco pero importante. La encripción se recomienda si se desea que los documentos se mantengan en secreto total, el tener los archivos encriptados nos permite agregar una capa mas de seguridad en caso de robo de archivos o disco duro. En estos casos se puede aplicar la encripción con algunos de los algoritmos mencionados en el capitulo 2, en el tema de Criptografía.

CONTROLES DE SOFTWARE

La seguridad computacional provee de medidas para prevenir y detectar acceso y uso no autorizado de equipo de computo. Para la primer configuración de sistemas propuestos se debe observar que debido a la falta de conexión a una red o Internet, no es posible que la seguridad sea violada por un pirata en línea (*hacker*). Por esta razón, diversas instituciones y empresas resguardan su información más critica en computadoras o terminales sin conexión a red alguna. Siendo así, la configuración 1 no se ve afectada por las vulnerabilidades de protocolos en línea y sistemas de archivos compartidos, los programas diseñados para la detección de intrusos tampoco tienen aplicación, los *firewall* tampoco son aplicados ni sistemas de autenticación como *Kerberos*. Sin embargo, aun hay amenazas para el sistema que no provienen de una red. Las siguientes recomendaciones en cuanto a controles de software son para elevar el nivel de seguridad de esta configuración.

PROGRAMAS AUDITORES. Los paquetes de monitoreo y auditoria se encargan de revisar la condición y la administración de los puntos de seguridad del sistema. En la configuración 1 de sistemas, estos paquetes no servirían para informar de riesgos en línea o vulnerabilidades debidas a una conexión externa, aunque si proporcionaran la siguiente información del sistema:

- Las vulnerabilidades que tendría el sistema si entra en línea y de actualizaciones recomendables.
- Una medición de la eficiencia en las operaciones, por ejemplo, cuantos virus fueron detectados vs cuantos fueron eliminados.
- Una evaluación del apego a las políticas de seguridad o estándares, por ejemplo, los estándares en antivirus especifican que todos los archivos ***.DAT***, donde se mantiene la información de nuevos virus, deben ser actualizados cada cierto tiempo.
- Establecimiento de las bases para un plan comprensivo de respuesta a incidentes de seguridad.

La información generada por los programas auditores puede almacenarse de varias formas: en archivos de lectura y escritura dentro de la terminal, en un dispositivo donde se escribe una vez y se puede leer varias (CD-ROM), o en un dispositivo de solo escritura (impresora de línea). Cada una de estos métodos tiene sus ventajas y desventajas. Si se opta por grabar los registros en un archivo de lectura-escritura dentro de la terminal se tendrá acceso instantáneo a los registros para su análisis en el momento deseado, por otro lado, es poco confiable ya que, si de alguna manera, alguien entra a esta terminal a robar información puede fácilmente borrar cualquier dato de la

intrusión al manipular los archivos del registro. La segunda opción es guardar la información en un medio de escritura única como un CD; esto es un poco más complicado de configurar, la información no estará disponible instantáneamente y el costo es más elevado, aunque es un metodo mas seguro porque un intruso no podra modificar los archivos en un CD. La tercera opción para el almacenamiento de la información de auditoria es con un dispositivo de solo escritura, una impresora de línea quedaría en esta categoría; este metodo es de mucha utilidad si se requieren registros permanentes e inmediatos para el caso donde se quiere saber el punto exacto de una falla o ataque al sistema; si se quiere usar una impresora laser o algun otro dispositivo que ponga la informacion en espera se puede perder la informacion en el momento critico; las desventajas de este metodo son el mantener alimentada con papel la impresora y donde guardar todo el papel utilizado para un análisis posterior. La información de los programas auditores puede ser clave para la investigación, detención y proceso legal de los responsables de robo informático.

PROGRAMAS ANTIVIRUS. Los virus informáticos pueden llegar de manera accidental o consciente a nuestro sistema, así que no se puede ignorar la peligrosidad de ellos para esta configuración. Enseguida se presentan recomendaciones de seguridad para tratar con la amenaza de virus:

- Utilizar solamente software adquirido de vendedores confiables y bien establecidos. Ciertamente existe el riesgo de recibir virus aun de grandes compañías de software, sin embargo estas compañías cuidan bien su reputación y son muy cuidadosas con los productos que sacan al mercado para que no contenga fallas o virus.
- En caso de que se deba usar software proveniente de fuentes de calidad y honradez desconocidas, se recomienda probar este nuevo software en una computadora distinta, que no contenga disco duro o disco de arranque. Se debe observar el comportamiento del software y buscar cualquier falla e indicios de actividad inexplicable en pantalla. Posteriormente hay que revisar la computadora de prueba con un programa detector de virus, diversos programas antivirus permiten crear un disco de detección. Solo después de pasar estas pruebas, el programa podrá ser instalado en nuestra estación de trabajo.
- Crear un disco de arranque y mantenerlo seguro. Es necesario mantener este disco contra escritura durante el reinicio del sistema. El disco debe de prepararse antes de que el sistema se infecte y tenerlo a la mano en cuanto surja la necesidad. Al usar el disco, los archivos del sistema (controladores, software de manejo de memoria) deben ser cargados desde el disco para asegurar que se inicia el sistema de manera confiable.
- Crear y conservar copias de respaldo de los archivos ejecutables del sistema. Así, en caso de una infección, los archivos afectados pueden ser removidos y reinstalados de las copias limpias.
- Utilizar detectores (*scanners*) de virus regularmente. Muchos de los detectores disponibles hoy en día permiten la detección y la eliminación de los virus. Se recomienda tener mas de un detector porque uno puede encontrar virus que otros ignoran. Los programas detectores buscan firmas conocidas de actividad viral, y están en constante actualización.

Los virus informáticos no se limitan a infectar un solo tipo de computadora o sistema operativo. Las PC son las más populares y por ello las que más sufren por virus, pero eso no significa que los propietarios de estaciones de trabajo de UNIX, LINUX, Macintosh estén exentos a estos riesgos. Los virus representan amenazas para cualquier programa almacenado sin protección contra escritura. Los sistemas operativos otorgan la opción de proteger los archivos contra escritura designándolos como "oculto" o "solo lectura", sin embargo, este tipo de protección puede ser superada por los programadores de virus fácilmente. Es erróneo pensar que nuestros archivos de información, listas, hojas de trabajo, etc. no serán infectados ya que los virus no se limitan a infectar los archivos de programa sino también afectan a los archivos de datos, esto lo logran al agregar a archivos de texto o de hojas de calculo ciertos comandos de inicio y así esparcen la infección o causan estragos. Si el sistema ha sido infectado hay ocasiones en que un simple apagado general y encendido de la maquina resuelve el problema ya que ciertos virus residen en memoria y al ser una memoria dinámica se pierde su contenido al quitar la energía,

aunque se debe tener en cuenta que este método no funcionara si el virus esta guardado en disco o si se encuentra ya en el sector de arranque. Se deben tener muchos cuidados para mantener un sistema funcional y al mismo tiempo protegido de los virus.

COPIAS DE RESPALDO. Es recomendable un mantenimiento periódico de todas las copias de respaldo del sistema, las cuales serán útiles si algunos de los programas utilizados o un virus causa problemas que obligan a la reinstalación del sistema. Con estas copias de respaldo también se deben tomar ciertas precauciones de seguridad, por ejemplo, los respaldos deben guardarse de preferencia fuera de la terminal pero que estén fácilmente disponibles para emergencias; estas copias de respaldo pueden ser encriptadas para mayor protección, sin embargo, hay que asegurarse de tener acceso rapido a los programas de desencripción.

CONTROL DE ACCESO Y AUTENTICACIÓN. Para un sistema que consta de una computadora sin conexión a Internet donde queremos tener información segura, podemos seguir las siguientes recomendaciones en cuanto a la instauración de un programa que controle los accesos a una terminal:

- La implementación de bitácoras de acceso a la computadora en conjunto con un proceso de autenticación de usuario por medio de palabras clave, así, en la bitácora quedara asentado quien tuvo acceso a la terminal, el día y la hora y las operaciones que llevo a cabo en ella.
- Dentro de los programas de acceso se puede implementar la característica de que los usuarios solo podrán acceder la terminal a cierta hora del día, teniendo un control total sobre quien esta usando la maquina a determinada hora.

El control de acceso considerara el proceso de autenticación de usuarios por medio de medidas de software, es decir, por medio del uso de passwords. La autenticación de los usuarios debe considerar varias situaciones: usuarios que escriban mal su passwords, malfuncionamiento del teclado, etc. Para el caso de uso de passwords ciertas medidas pueden ser programadas por dentro del programa controlador de accesos:

- Implementar un pequeño retardo en el proceso de verificación de 5 a 10 segundos. Para un usuario normal este proceso presentara un mínimo de molestia, sin embargo, para un posible ladrón de información que use programas de ataque por búsqueda en diccionario, este retardo en cada intento de introducción de un password para que el ataque sea infeasible.
- Determinar el número de intentos de passwords equivocados que puede hacer un usuario. En caso de que sea muy importante para el negocio mantener ladrones fuera del sistema, con tres oportunidades basta. Si se dan las tres entradas equivocadas, la cuenta del usuario debe ser dada de baja y solo el encargado de seguridad puede volver a habilitarla. Esto facilita la identificación de cuentas que están bajo ataque o en peligro por perpetradores.
- Programar el sistema para que obligue a los usuarios a cambiar de password periódicamente. Para evitar el reuso de passwords algunos sistemas de control de acceso rechazan cualquiera que haya sido usada recientemente.

Una técnica muy recomendable en el uso de passwords es utilizar las de "uso único" (*one-time password*). Estas cambian cada vez que son usadas. En estos passwords al usuario se le asigna no una frase, sino una función matemática. Aquí el sistema da un argumento para la función y el usuario debe introducir el valor resultante. Un sistema que utilice este técnica es llamado desafío-respuesta (*challenge-response*) porque el sistema le presenta al usuario un desafío y determina la autenticidad del usuario por su respuesta. Las funciones que se definen para los passwords de uso único pueden llegar a ser muy complejas, por ejemplo: $f(E(x))=E(D(E(x))+1)$ en donde la computadora envía un valor encriptado $E(x)$ y el usuario debe desencriptar el valor, aplicar la función aritmética $+1$ y encriptar el nuevo resultado para enviarlo de regreso al sistema. Los passwords de uso único son muy seguros ya que si descubren uno, este es inútil.

Estas recomendaciones son hechas pensando en que solo se debe desconfiar del usuario, pero existe el caso en que el sistema ya haya sido comprometido. Es muy sencillo crear un programa que muestre o simule el símbolo del sistema y los espacios para el ID del usuario y el password, capture la información escrita y la guarde. En este tipo de ataque el perpetrador escribe el programa, lo coloca en la terminal, espera que alguien escriba su password y se aleja sin que nadie se de cuenta. Las recomendaciones para evitar este tipo de ataque son:

- Asegurarse de siempre reiniciar la ruta al sistema. En algunos sistemas el presionar la tecla BREAK detiene los procesos que se realizan, o proceder al apagado y encendido de la terminal.
- Para asegurarse que la computadora esta corriendo el sistema que se desea, podemos programar el control de acceso para que antes de introducir el password o datos confidenciales, muestre la fecha de la ultima vez que el usuario entró al sistema. Si se desea un mayor nivel de seguridad se puede encriptar el mensaje con la fecha, y el usuario se encargara de desencriptar y verificar la información, si es correcta el usuario encripta la fecha y el password para garantizar que un intruso no la haya interceptado. Estas encripciones y desencripciones pueden ser hechas con algoritmos del tipo DES.

Varias compañías de software se dedican a desarrollar sistemas de control de acceso. Estos paquetes proveen de autenticación de usuario, limitación en los accesos y bitácora de registro, por ello es recomendable su utilización ya que la seguridad del sistema se ve beneficiada con estas funciones.

CONTROLES DE HARDWARE

BIOS. Para la primer configuración que representa una sola computadora hay un método básico para la seguridad, el cual es proporcionado por el BIOS, la EEPROM de las computadoras que contiene los datos de configuración y de información del sistema. El orden de los dispositivos de arranque, controlado por el BIOS, es causa de preocupación porque casi todos los sistemas operativos tratan de arrancar primero desde la unidad de discos, después desde la unidad de CD o del disco duro. Si se deja que persista la configuración donde se busca primero en la unidad de disco, alguien podría aprovecharlo y reiniciar el sistema desde un disco que contiene código ejecutable. Para la eliminación de esta vulnerabilidad, hay que configurar el BIOS para que arranque desde el disco duro desde la primera vez, y si es posible, eliminar la unidad de disco y el CD-ROM de la secuencia. Posteriormente agregar una protección por password al BIOS. Esto obliga a que se introduzca el password antes de permitir hacer cambios al BIOS. Con ello se evita que alguien vuelva a cambiar la secuencia de arranque para usar la unidad de disco, al mismo tiempo protege de alguien que intente evitar el inicio del sistema. Sin embargo, sigue siendo muy sencillo evadir la protección de palabra clave en el BIOS. Solo se debe cambiar la posición de un jumper en la tarjeta madre (*motherboard*) y así la configuración del BIOS volverá a su estado por default deshaciéndose de la palabra clave. La protección del BIOS depende de los conocimientos que tenga en cuanto a computadoras el atacante y del trabajo que cuesta mover el jumper, ya que hay que abrir la computadora y localizar el jumper. Esto afecta a todos los sistemas operativos ya que el BIOS es parte de la arquitectura de la PC.

En caso de utilizar el sistema LINUX, se puede aplicar el Linux Loader (LILO), esté se coloca en el registro del *master boot* del sistema. El BIOS busca al iniciar un dispositivo *bootstrap* ejecutable y LILO actúa como tal. Al encontrarlo BIOS le cede la ejecución a LILO. LILO cargara el *kernel* de LINUX, y este completara el proceso de arranque. LILO permite que se arranque el sistema en un cierto estado de operación ***init***. Aquí aparece un problema de seguridad, ya que cuando un usuario desea arrancar en el estado 1 (***init state 1***) el requisito de la autenticación es pasado por alto, y se presenta la línea de comandos de la consola con privilegios de raíz. Para evitar este problema, se puede agregar una protección por password a la configuración de LILO, la cual se encuentra en el archivo ***/etc/lilo.con***. De esta manera será necesario introducir el password cada que se desee arrancar un sistema operativo, o incluso usar un password distinto para cada sistema operativo disponible. Para prevenir que los usuarios vean la información del archivo, se configuran los permisos para que solo se puedan leer desde raíz.

SMARTCARD. Para la primer configuración hay otra opción para protección de la computadora, es la smartcard (tarjeta inteligente), la cual genera cada determinado tiempo un password que permite el acceso hacia las áreas de la información critica de la PC, o para utilizar la estación de trabajo. Si no se tiene el password o la smartcard, el acceso es prácticamente imposible, ya que el password que genera esta formado por letras y números de distinta longitud, obligando a un ataque largo y tedioso con programas de fuerza bruta. Muchos negocios utilizan técnicas de autenticación biométrica en conjunto con smartcards; de las técnicas biométricas se habla detalladamente en el apartado de **Controles Físicos**, solo se mencionara que las técnicas biométricas miden alguna característica física única del usuario, tal como el patrón de la voz, de cara, el orden de los vasos sanguíneos de la cornea y las huellas digitales. Tradicionalmente, las representaciones digitales de las características biométricas ocupan un espacio entre 100 y 600 bytes y por ello se pueden acomodar en una smartcard. Los pasos tipicos de una autenticación de usuario por medio de smartcard y medidas biométricas son los siguientes:

1. Insertar la smartcard en el lector, esta contiene las llaves criptográficas y los datos correspondientes a la huella digital del usuario.
2. Se introduce el número de identificación privada (PIN), así, se libera la representación electrónica de la huella digital.
3. Ahora se coloca el dedo en el escáner, esta huella es comparada con la guardada en la smartcard.
4. Si la comparación es positiva, los datos de la huella en la smartcard son convertidos a un valor numérico y se combinan con el PIN de la smartcard para formar una llave de encripción simétrica la cual desencripta la llave privada.
5. Un número aleatorio es generado por la computadora donde se conecta la smartcard, este número es transferido a la smartcard.
6. La llave privada en la smartcard es usada para encriptar el número aleatorio y mandarlo de vuelta a la computadora.
7. La computadora verifica que una llave pública certificada obtenida de algún directorio en red desencripte el número aleatorio y verifica que este sea el mismo que se envió originalmente a la smartcard.

Este proceso se encarga de autenticar de manera irrefutable al usuario de la smartcard.

PUERTOS INFRARROJOS. Muchas de las computadoras portátiles vienen equipadas con puertos infrarrojos, los cuales permiten la comunicación inalámbrica entre dos computadoras o con agendas portátiles (palms). Estos puertos son vulnerables a intentos de acceso, robo de información o causar un sobreflujo del buffer y la aparición de la pantalla azul y reinicio del sistema. Para evitar esto se pueden tomar las siguientes medidas:

- Descargar los parches y actualizaciones que cubran esta vulnerabilidad y que ya están disponibles.
- También hay que deshabilitar los dispositivos infrarrojos si no están en uso, no basta con deshabilitar la comunicación, sino que hay que deshabilitar todo el dispositivo utilizando el programa Administrador de Dispositivos.
- Asegurarse que los puertos infrarrojos tienen bloqueada la línea de vista.

También se puede colocar cinta opaca sobre el puerto aunque esto solo servirá si el oponente no tiene acceso a la máquina.

POLÍTICAS

Si no hay políticas de seguridad es muy probable que el sistema sea comprometido. Es conveniente que antes de enunciar políticas dentro del negocio o compañía se creen los lineamientos de uso, se haga un análisis de riesgos en el sistema y se establezca una estructura para el equipo de seguridad. Los lineamientos de políticas deben encargarse de contestar unas preguntas: A QUIEN se le permite acceso? A QUE recursos? y COMO se regula el acceso?. Las

políticas también deben especificar: las metas en seguridad de la organización, quien tiene la responsabilidad de la seguridad, y el compromiso de la organización con la seguridad. En esta configuración se tiene una computadora sin conexión a una red o Internet, se pueden imponer las siguientes políticas, aunque esto depende de las necesidades de seguridad del negocio ya que las políticas se pueden hacer más restrictivas o más libres.

- Cada determinado tiempo hacer obligatorio el cambio de password para inicio del sistema.
- No utilizar el nombre propio o apellido como clave de acceso, ni el nombre de la pareja, hijo o mascota, tampoco el número telefónico, número de licencia, marcas de autos, direcciones o nombres de calles.
- Cada cierto tiempo el encargado de esta computadora o de la seguridad del sistema debe de respaldar la información de mayor importancia.
- Indicarle a los usuarios del sistema que no deben escribir sus passwords en ninguna lista o papel.
- Instruir a los usuarios para utilizar distintos passwords para cada aplicación o inicio del sistema.
- Los usuarios del sistema deben utilizar caracteres alfabéticos y numéricos (por ejemplo K87cvE) para la elaboración de sus claves de acceso al sistema o de inicio del sistema.
- No revelar a gente no autorizada las claves de acceso.
- No abandonar de la estación de trabajo dejándola encendida.
- La firma de cláusulas explicitas dentro de los contratos de los trabajadores en donde acepten no revelar información a competidores. Así se puede emprender acción legal en caso de que lo anterior suceda.

Las políticas de seguridad son reglas que nos dictan como conservar la seguridad y las acciones a tomar en caso de una ruptura a la seguridad e incursión dentro de la máquina que se quiere proteger.

CONTROLES FÍSICOS

AUTENTICACIÓN BIOMÉTRICA. Para la configuración 1 de los sistemas informáticos existen algunas medidas físicas llamadas biométricas (*biometrics*) para evitar el acceso a computadoras o a los edificios y oficinas contienen estas computadoras y al mismo tiempo para proteger la información contenida dentro de estos sistemas. Se pueden emplear los siguientes métodos de protección:

- Revisión de retina
- Las técnicas de reconocimiento de voz y de firma de usuario, aunque estas no son biométricas
- Técnicas de autenticación de rostro, mano o huellas digitales

El uso y aplicación de estas técnicas depende de evaluar previamente varios factores: nivel de seguridad que se necesite, costo y tiempo de implementación, aceptación de los usuarios y confiabilidad.

- Nivel de seguridad. El reconocimiento de voz y de firma son técnicas aceptables cuando se habla de usos no relacionados con autorización de acceso a la PC, sin embargo son útiles para la autenticación de usuarios de PC. Las técnicas biométricas que identifican características físicas son más confiables y otorgan un nivel mayor de seguridad.
- Costo y tiempo de implementación. Cuando se desea implementar un sistema de autenticación biométrica de usuario, se debe de hacer en conjunto con el proveedor de computadoras y tomar en cuenta que hay que buscar e instalar el software y hardware compatible con la PC para autenticación (cámaras, lectores, scanners), el software y hardware necesarios para mantener la base de datos de usuarios, el tiempo que se lleva integrar el hardware de autenticación en el ambiente de trabajo, el entrenamiento del staff para manejar el nuevo sistema, el entrenamiento de los usuarios con el nuevo protocolo de autenticación y la actualización continua de las bases de datos.

- Aceptación de usuarios. Los usuarios generalmente aceptan las técnicas que son menos intrusivas o gorrosas, tales como identificación de huellas, rostro o mano. Aquí es responsabilidad de la organización el entrenar a los empleados para que se familiaricen con los nuevos requerimientos antes de que el sistema sea implementado.
- Confiabilidad. La revisión de retina e identificación de iris son altamente eficientes para identificar individuos, sin embrago, son muy costosas y la mayor parte de los negocios no necesitan este nivel de confiabilidad. Las técnicas de autenticación de huellas, mano, y rostro ofrecen buena confiabilidad, los cambios físicos tales como cortadas, cicatrices y el envejecimiento pueden afectar la identificación, sin embargo las bases de datos se pueden actualizar.

Existen dos términos que describen la funcionalidad de las técnicas biométricas: la razón de falsa aceptación (False Aceptance Rate, FAR) que es la probabilidad de que un intruso sea aceptado con una medida que no le pertenece de un usuario enrolado. La razón de rechazo falso (False Rejection Rate, FRR) es la probabilidad con que un usuario enrolado sea rechazado. Se considera que un buen equipo biométrico tiene un bajo FRR y FAR. Casi siempre hay un intercambio entre seguridad y conveniencia, en los sistemas biométricos mientras más seguro el sistema (mas bajo FAR) es más inconveniente para el usuario, ya que ocurren más rechazos falsos. Similarmente, mientras más conveniente sea el sistema, menos seguridad tiene. Los sistemas biométricos le permiten al usuario elegir entre un amplio rango de niveles de FAR/FRR.

Tomando en cuenta que puede haber ocasiones extremas en donde se utilice un dedo cortado de la mano o dedos falsos, algunos dispositivos miden el calor del dedo en el escáner y otros miden su conductividad para evitar casos donde se modifiquen las huellas con silicón. La solución más adecuada es por medio de la medición **espectroscópica** de la cantidad de hemoglobina oxigenada en la sangre, ya que es imposible de pasar con dedos artificiales y los resultados de esta prueba son muy distintos para dedos vivos y dedos cortados.

HERRAMIENTAS Y MEDIDAS FÍSICAS. Dentro de los controles físicos se deben considerar también las estrategias y herramientas que ayudan a impedir los incidentes de robo y perdida de equipo de computo. Los perpetradores de esto pueden ser simples oportunistas, ladrones, criminales de carrera, bandas organizadas, gente en contacto con los productos e individuos que trabajan en el ambiente afectado. Reforzar el blanco (*target hardening*) es un proceso de edificar una serie de barreras físicas para desalentar el progreso de un adversario, con el reforzamiento se pretende que el atacante renuncie a la idea antes de atacar, se rinda durante el ataque o demorarlo lo suficiente para que una fuerza de respuesta se encargue del ataque antes de que sea completado. Para minimizar esta amenaza pueden emplearse las medidas descritas a continuación:

- Designar un oficial de seguridad departamental, quien reportara rupturas en la seguridad y actos ilegales. Además será el responsable de implementar, coordinar, mantener y monitorear un programa de seguridad departamental.
- Instalar puertas y ventanas que den entrada al edificio u oficina donde esta la computadora a proteger que cuenten con alarmas contra apertura o ruptura.
- Monitorear el perímetro del edificio o las oficinas donde se encuentra la computadora resguardada con cámaras de circuito cerrado.
- Organizar un patrullaje de seguridad llevado a cabo por guardias.
- Establecer puntos de recepción en el edificio, entre áreas funcionales o zonas seguras.
- Definir claramente los limites del acceso público en el edificio, por medio de señalamientos.
- Para proteger una computadora de escritorio, se puede colocar el monitor, teclado, impresora y CPU en un gabinete bajo llave. En caso de una laptop se puede utilizar un gabinete más pequeño.
- Se puede colocar una alarma dentro de la PC, con esto no se evita el robo pero generalmente ahuyenta a los agresores.

- Los cables de aseguramiento de computadoras son muy populares hoy en día y pueden ser otra opción en lugar del gabinete, así como placas de acero para aseguramiento que mantienen la computadora junto a la mesa.
- Para evitar el acceso a las unidades de disco de la computadora se emplean candados con llave.

NIVEL DE SEGURIDAD

En la configuración uno se tiene una computadora sin conexión a red alguna. Antes de aplicar las recomendaciones, el nivel de seguridad es apenas de **1** si el sistema cumple con protección antivirus y protecciones contra robo físico.

El sistema tiene así una buena operatividad:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{1} = 1$$

Con las recomendaciones hechas en los apartados de **Encripción, Controles de Software, Controles de Hardware, Políticas** y **Controles físicos** se cubren las características descritas para la obtención del nivel **3** de seguridad. Este nivel sería el mayor para equipos sin conexión a Internet, ya que esta configuración no requiere de protección contra accesos desde Internet, y como no es una red tampoco requiere detección de actividad inusual.

Su nivel de operatividad esta determinado por la formula:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{3} = 0.333$$

El nivel de operatividad es intermedio, no es muy alto ya que se aplican varias herramientas de seguridad, esto permite que sea accesible y rápida la operación, aunque no a un nivel tan alto como cuando el sistema tiene sus características de seguridad por default.

Tabla 4.2 - Niveles de Seguridad y Operatividad

Nivel de seguridad por default	**1**
Nivel de Operatividad por default	**1**
Nivel de Seguridad con recomendaciones	**3**
Nivel de Operatividad con recomendaciones	**0.3333**

Las descripciones hechas para los niveles del Orange Book en la página 22 pueden usarse para saber en que nivel queda el sistema de la configuración uno después de aplicarle las recomendaciones de seguridad, con una correcta implementación de las políticas y control de accesos. Se cubren los requisitos aproximados para el nivel **B1** junto con algunas características del nivel **B3** y **B2**. El nivel B2 indica la etiquetación de objetos con un nivel de seguridad y objetos con un nivel diferente; así que esto depende del tipo de recursos que se manejen y como estén organizados. Aun así, el sistema muestra un nivel de seguridad muy alto, suficientemente seguro para que diferentes usuarios trabajen en él, sin haber fuga de información.

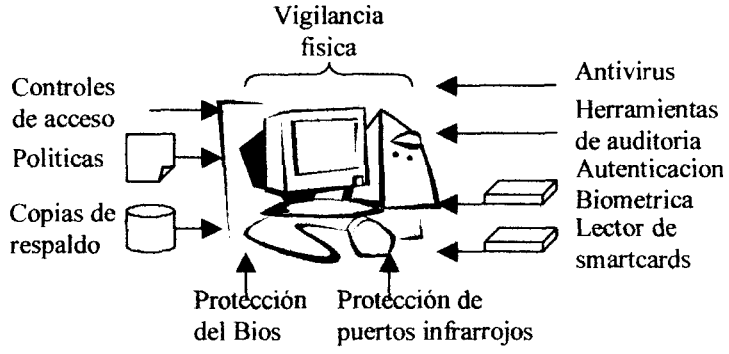


Figura 4.3 - Configuración protegida

CONFIGURACIÓN 2 - Una sola computadora con conexión a Internet

En la configuración dos se tiene una computadora con conexión a Internet. Los pasos que se toman para lograr un buen nivel de seguridad y privacidad informática son, en general, similares a los de la configuración uno. Las características por default de seguridad de una terminal con conexión a Internet consisten en: un sistema operativo sin sus parches de seguridad instalados, ningún tipo de autenticación de usuario o codificación para proteger archivos importantes, sistemas de archivos vulnerables a falsificación de datos, ningún software de auditorias, ni programas o dispositivos para evitar incursiones al sistema desde Internet o detectores de intrusos, además de que casi todas las características de seguridad de los sistemas operativos están puestas al mínimo por default. Muchos de los equipos de computo vienen de fabrica con programas antivirus instalados (aunque no necesariamente actualizados) y candados o elementos de seguridad física. La seguridad por default, para esta configuración es deficiente.

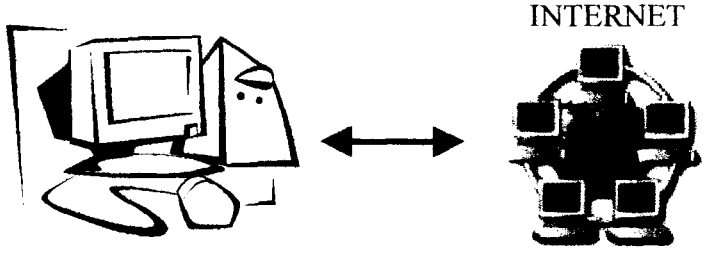


Figura 4.4 - Una sola computadora con conexión a Internet

ENCRIPCIÓN

El uso de la encripción es aconsejable. La encripción se puede aplicar para la protección de información de respaldo del sistema, y en conjunto con los protocolos de seguridad como se explica en el apartado de **Controles de Software**.

CONTROLES DE SOFTWARE

Para esta configuración se deben considerar que debido a la conexión a Internet se tienen vulnerabilidades causadas por piratas en línea, programadores de virus, gusanos (*worms*), caballos de troya (*trojan horse*), puertas traseras (*backdoors*) y otras amenazas que utilizan como medio de transmisión Internet. Y no hay que olvidar las vulnerabilidades de la configuración 1.

PROGRAMAS AUDITORES. Los paquetes de monitoreo y auditoria se encargan de revisar la condición y la administración de los puntos de seguridad del sistema. En la configuración dos de sistemas, estos paquetes serian muy útiles, proporcionando la siguiente información del sistema:

- Las vulnerabilidades que tiene el sistema al estar en línea y de actualizaciones recomendables para los distintos programas que contiene nuestro equipo. Ya que cualquiera de ellos puede representar un problema de seguridad al entrar en línea por la gran variedad de código dañino que nos podemos encontrar al explorar la red.
- Una medición de la eficiencia en las operaciones, por ejemplo, cuantos virus fueron detectados vs cuantos fueron limpiados.
- Una evaluación del apego a las políticas de seguridad o estándares, por ejemplo, los estándares en antivirus especifican que todos los archivos ***.DAT***, donde se mantiene la información de nuevos virus, deben ser descargados cada cierto tiempo.
- Establecimiento de las bases para un plan comprensivo de respuesta a incidentes de seguridad.

La información generada por los programas auditores puede almacenarse de varias formas: en archivos de lectura y escritura dentro de la terminal, en un dispositivo donde se escribe una vez y se puede leer varias (CD-ROM), o en un dispositivo de solo escritura (impresora de línea). Cada una de estos métodos tiene sus ventajas y desventajas. Si se opta por grabar los registros en un archivo de lectura-escritura dentro de la terminal, se tendrá acceso instantáneo a los registros para su análisis en el momento deseado, por otro lado, es poco confiable ya que, si alguien logra acceder a este sistema por la conexión a Internet o por un método distinto y su intención es robar información, modificarla, o falsificarla, al mismo tiempo puede borrar cualquier dato de la intrusión al manipular los archivos del registro. La segunda opción es guardar la información en un medio donde se escriba una vez, como un CD; esto es un poco más complicado de configurar, la información no estará disponible instantáneamente y el costo es más elevado, aunque es un método mas seguro ya que, un intruso no podrá modificar los archivos en un CD para cubrir su intrusión. La tercera opción para el almacenamiento de la información de auditoria es con un dispositivo de solo escritura, una impresora de línea quedaría en esta categoría; este método es de mucha utilidad si se requieren registros permanentes e inmediatos para el caso donde se quiere saber el punto exacto de una falla o ataque al sistema; si se quiere usar una impresora láser o algún otro dispositivo que ponga la información en espera se puede perder la información en el momento critico; las desventajas de este método son el mantener alimentada con papel la impresora y donde guardar todo el papel utilizado para un análisis posterior. La información de los programas auditores puede ser clave para la investigación, detención y proceso legal de los responsables de robo informático. Algunos ejemplos de programas que sirven para hacer auditorias de seguridad son: ***LT Auditor+ versión 8.0, Nessus, Nmap***.

PROGRAMAS ANTIVIRUS. En esta segunda configuración de sistemas, los virus informáticos están presentes y pueden llegar de manera accidental o intencional a nuestro equipo, ya sea por medio de un archivo enviado, por correo electrónico o simplemente al abrir alguna página web. Es por ello que se presentan recomendaciones de seguridad para tratar con la amenaza de los virus:

- Utilizar solamente software adquirido de vendedores confiables y bien establecidos.
- En caso de que se deba usar software proveniente de fuentes de calidad y honradez desconocidas, se recomienda probar este nuevo software en una computadora distinta, que no contenga disco duro ni disco de arranque. Se debe observar el comportamiento del software y buscar cualquier falla e indicios de actividad inexplicable en pantalla. Posteriormente hay que revisar la computadora de prueba con un programa detector de virus, diversos programas antivirus permiten crear un disco de detección.
- Crear un disco de arranque y mantenerlo seguro. Es necesario mantener este disco protegido contra escritura durante el reinicio del sistema. El disco debe de prepararse antes de que el sistema se infecte y tenerlo a la mano en cuanto surja la necesidad.

- Crear y conservar copias de respaldo de los archivos ejecutables del sistema. Así, en caso de una infección, los archivos afectados pueden ser removidos y reinstalados de las copias limpias.
- Utilizar detectores (*scanners*) de virus regularmente. Muchos de los detectores disponibles hoy en día permiten la detección y la eliminación de los virus. Se recomienda tener mas de un detector porque uno puede encontrar virus que otros ignoran. Estos programas generalmente pueden actualizarse en línea, descargando nuevas definiciones de virus.
- Es una practica popular el enviar virus disfrazados de correo electrónico, por lo que no es recomendable abrir correos de personas desconocidas.
- Ciertas páginas de Internet creadas por piratas o modificadas por ellos, pueden causar la contaminación por virus de modo que lo recomendable es no abrir páginas que presenten riesgo de este tipo, o si existe la necesidad de ello, primero activar la protección en tiempo real que ofrecen los programas antivirus, al mismo tiempo que se aumenta el nivel de seguridad en el explorador para que impida que se graben archivos en el disco duro sin el consentimiento del usuario.

Las amenazas por virus informáticos no infectan un solo tipo de computadora o sistema operativo. Las PC son las más populares y por ello las que más sufren por virus, pero eso no significa que los propietarios de estaciones de trabajo de UNIX, LINUX, Macintosh estén exentos a estos riesgos. Los virus representan amenazas para cualquier programa almacenado sin protección contra escritura. Los sistemas operativos otorgan la opción de proteger los archivos contra escritura designándolos como "oculto" o "solo lectura", sin embargo, este tipo de protección puede ser superada por los programadores de virus fácilmente. Es incorrecto pensar que los archivos de información, listas, hojas de trabajo, etc. están a salvo de ser infectados, los virus no solo se limitan a infectar los archivos de programa sino también afectan a los archivos de datos, esto lo logran al agregar a archivos de texto o de hojas de calculo ciertos comandos de inicio y así esparcen la infección o causan estragos. Si el sistema ha sido infectado hay ocasiones en que un simple apagado general y encendido de la maquina libra del problema ya que ciertos virus residen en memoria y al ser una memoria dinámica se pierde su contenido al quitar la energía, aunque se debe tener en cuenta que este método no funcionara si el virus esta guardado en disco o si se encuentra ya en el sector de arranque. Se deben tener muchos cuidados para mantener un sistema funcional y al mismo tiempo protegido de los virus.

FIREWALLS. Una manera muy popular y efectiva de prepararse contra intrusiones por Internet es por medio de *firewalls*. Para la configuración dos, un firewall nos permite proteger todos los elementos conectados a nuestra terminal, ya sean los lectores de tarjetas, impresoras, scanners, etc. El *firewall* es un proceso que filtra el trafico entre la computadora y la red exterior, esto lo hace al aplicar ciertas políticas, como puede ser evitar el acceso del exterior y alternativamente permitir el acceso al exterior de ciertas aplicaciones. Parte del reto de instalar un *firewall* es definir de manera apropiada para las actividades de nuestro sistema las políticas en que se basara el filtrado. Existen tres dispositivos que responden al nombre de *firewall*: un *screening router*, el *proxy gateway*, y el *guard*. En general los *screening routers* tienden a implementar políticas de seguridad simplistas, mientras que los *guards* y *proxy gateways* tienen un conjunto mayor de opciones para políticas de seguridad.

Para la configuración dos de sistemas la opción mas adecuada a aplicar sería un tipo de *firewall* personal. Es decir, que solo protege a la computadora en que esta instalado. ***Symantec*** provee software de *firewall* personal y este se basa en definir de que sitios en línea acepta paquetes, de que sistemas de archivos acepta paquetes y que políticas de seguridad aplicara para proteger la computadora conectada a Internet.

En caso de tener suficientes recursos se puede optar por usar el *proxy gateway* ya que éste simula los efectos de una aplicación, evitando que la terminal detrás del *firewall* reciba peticiones para actuar erróneamente. El *gateway* corre semi-aplicaciones, simula ser el interior para el exterior y viceversa.

Hay que recordar que un *firewall* no protege a los datos que salen del ambiente protegido. Además de que para los piratas o *crackers* que navegan en la red, el *firewall* es el elemento visible hacia el exterior y por tanto puede atraer atacantes, por eso se recomienda no confiar en un solo *firewall*, si realmente se quiere tener medidas de seguridad fuertes se pueden instalar diferentes capas de protección llamadas ***defense in depth***. Los *firewalls* pueden resistir ataques pero no son impasables, por esto los diseñadores los mantienen pequeños para no dar herramientas extras a un atacante. Es muy importante configurar correctamente los *firewalls*, esa configuración debe ser actualizada si cambia el ambiente interno del *firewall* y lo recomendable es que los reportes de actividades del *firewall* sean revisados periódicamente. Los *firewalls* tienen poco control sobre el contenido que se admite dentro del ambiente así que este debe ser controlado por otras herramientas de seguridad.

PROTOCOLOS. En esta configuración tenemos una conexión a Internet, lo que significa que podremos enviar y recibir información a través de la red. En este apartado de controles de software agregamos recomendaciones de seguridad al usar los protocolos o sistemas de transferencia de archivos por Internet.

- **FTP**. El protocolo de transferencia de archivos permite a un usuario transferir archivos de texto o binarios entre dos computadoras en red por medio de los puertos 20 y 21. La conexión entre dos computadoras también puede darse por Internet. El protocolo FTP utiliza una estructura cliente-servidor con un programa cliente abriendo una sesión en un servidor. Existen muchos servidores anónimos en Internet que le permiten a uno descargar información sin necesidad de autenticarse. Si este mismo servidor permite la grabación de archivos entonces puede ser utilizado para distribuir software ilegal o dañino. Un servidor de este tipo podría ser fuente de virus, troyanos o gusanos informáticos, es por ello que solo se debe permitir el uso del protocolo a las aplicaciones que usen ftp con los puertos correctamente especificados a través del firewall de la red. Debe tenerse cuidado con la información descargada de un servidor, y se recomienda revisarla con programas antivirus siempre y en la medida de lo posible probar antes el software descargado en una computadora distinta a la principal.
- **GOPHER**. Gopher es un sistema cliente-servidor diseñado para localizar y recuperar archivos o información desde servidores por toda Internet. Los tipos de datos recuperados pueden ser archivos de gráficos o texto, programas script y archivos binarios ejecutables. Si estos archivos son recuperados y ejecutados sin que el usuario lo analice es posible que se obtenga y ejecute código dañino (virus o caballos de Troya). Por esto se recomienda que al usar Gopher la información recuperada sea revisada con programas antivirus antes de ser ejecutada.
- **ICMP**. El protocolo de mensaje de control de Internet es utilizado para determinar la información de ruteo y el estado de anfitrión (*host*). Un paquete de redirección ICMP es utilizado para informar a un ruteador o computadora sobre "nuevas y mejores" rutas hacia un destino. Estos paquetes pueden ser falsificados para dar rutas falsas hacia un destino y permitir a un atacante entrar a un sistema. Otro paquete común de ICMP es conocido como "mensaje inalcanzable". Este paquete señala problemas con una ruta a una dirección destino. Si se falsifica un mensaje de este tipo se puede causar la negación de acceso a otra red o anfitrión (*host*). Para proteger el sistema de esta vulnerabilidad se puede configurar el servidor de ruteo o el *firewall* para ignorar los "mensajes inalcanzable" ICMP. "PING" es un servicio ICMP el cual envía un paquete a un destino dado preguntando si "¿esta vivo?", La dirección destino regresa una afirmación o un "mensaje inalcanzable" ICMP. Lo recomendable al usar este servicio es filtrar los paquetes ICMP y no permitirles el acceso a través de los limites del sistema.
- **RPC**. Una llamada a procedimiento remoto (RPC) es similar a una llamada a procedimiento en C. La diferencia es que una RPC incluye una dirección IP remota y un puerto. El procedimiento es llamado en una computadora y ejecutado en otra. Estas llamadas a procedimiento y los puertos pueden ser usados por un pirata informático para obtener

acceso no autorizado a los recursos e información sobre un sistema. La recomendación es que las llamadas remotas a procedimientos deben ser filtradas e impedirles el acceso a través del sistema. Aunque existe el problema de que algunas aplicaciones de Windows requieren de RPC para seguir operando, por lo que se deben abrir numerosos puertos para apoyar la funcionalidad de RPC, causando numerosos y serios problemas de seguridad.

- **Windows X**. Xwindows es un ambiente grafico para el software de aplicación de usuario. Este ambiente soporta servicios distribuidos usando puertos TCP y esta diseñado para controlar y mostrar de manera remota procesos a través de la red. En este sistema existe el riesgo de que un proceso dañino tome control o vigile la pantalla, el teclado y mouse. La necesidad de abrir muchos puertos le da a un intruso la oportunidad para usar un puerto abierto y comprometer un sistema confiable con una conexión vulnerable. Al usar este ambiente se recomienda usar un programa que vigile la detección de intrusos en el sistema, así como un antivirus con protección en tiempo real. No debe permitírsele el paso a través del *firewall* a información del sistema Xwindows
- **DNS**. El sistema de nombres de dominio (DNS) es un método jerárquico y distribuido de organizar el espacio de nombres en Internet, se encarga de darles nombre a las direcciones de IP. Utilizando este sistema, un *host* hace una petición con un datagrama de protocolo de usuario (UDP) a un servidor DNS. Las peticiones también pueden hacerse con TCP (en el puerto 53) y se les da el nombre de transferencias de zona. Las transferencias de zona pueden ser usadas por piratas para obtener listas de posibles blancos. Se recomienda que el acceso a este puerto sea permitido solo a servidores secundarios de dominio conocidos.
- **E-mail**. Electronic mail es una de las aplicaciones más usadas en Internet. Los mensajes son transportados utilizando un formato especifico para ellos junto con el protocolo de transporte para el correo simple (SMTP). Los mensajes de correo electrónico pueden ser leídos, modificados y falsificados muy fácilmente. Lo recomendable para agregar un mejor nivel de seguridad es aplicar un algoritmo de criptografía al mensaje antes de enviarlo, para garantizar la integridad del mensaje y autenticidad de su origen se utiliza la firma digital.
- **SMTP**. El protocolo de transporte para el correo simple (SMTP) es un protocolo en el nivel de aplicación utilizado para distribuir mensajes de correo electrónico entre computadoras. Este protocolo es muy simple y entiende solo mensajes y comandos basados en texto simple. SMTP no ofrece ningún método para verificar la fuente del mensaje o para garantizar la integridad del mensaje, en caso de utilizar este protocolo se recomienda usar en conjunto a un nivel mas alto el protocolo PEM.
- **PEM**. El correo de privacidad mejorada (PEM) es un conjunto de estándares para agregar seguridad al correo electrónico de Internet. Este conjunto de estándares describe un protocolo de seguridad que puede ser utilizado encima del SMTP o del protocolo ***Unix-to-Unix Copy Protocol*** (UUCP). PEM provee tres servicios de seguridad: integridad, autenticación del origen, y confidencialidad. PEM define un algoritmo de encripción asimétrica para la administración de llaves y operaciones de firma digital, y un algoritmo de encripción simétrica para encripción del mensaje.
- **PGP**. El paquete de encripción de muy buena privacidad (PGP) hace uso de encripción por llave pública para proteger correo electrónico y archivos de datos. Permite la comunicación segura con desconocidos, sin necesidad de canales seguros para un intercambio de llaves. Da un servicio rápido, con un sofisticado manejo de llaves, firmas digitales, compresión de datos. PGP usa el algoritmo RSA para el manejo de llaves y firmas digitales, y usa el algoritmo IDEA para proveer de confidencialidad.
- **MIME**. Las extensiones multipropósito de correo de Internet (MIME) fueron creadas por la Fuerza de Tarea de Ingeniería de Internet (IETF) como una solución que le permite a los usuarios adjuntar objetos cuyo formato no es texto a los mensajes de Internet. Algunos de los programas de correo electrónico MIME le dan al usuario la opción de configurar el tipo de datos adjuntos que son aceptados, y como ser interpretados, siendo muy importante

para evitar que ciertos datos adjuntos se ejecuten e interpreten de manera automática, así se evita que virus o gusanos se introduzcan en nuestro equipo por este medio.

- **HTTP**. El protocolo de transferencia de hipertexto (http) es un protocolo a nivel aplicación utilizado para acceder a la red de cobertura mundial (www). Este protocolo transfiere un bloque de información y una descripción del tipo de datos al programa cliente (Internet Explorer, Netscape Navigator, Lynx, Mosaic), y este se encarga de interpretar la información para presentarla al usuario de forma correcta. El recibir código ejecutable es una actividad normal con este protocolo, por lo que se debe cuidar el configurar los programas cliente para preguntar antes de ejecutar cualquier *script* o código y revisar con programas antivirus cualquier código ejecutable descargado. Algunos sitios en Internet utilizan el protocolo https que es una versión segura del http, donde se agregan las cualidades del PEM sobre http para encriptar y autenticar el mensaje.
- **IPSec**. IPsec es el protocolo estándar para la aplicación de confidencialidad, autenticación e integridad en la capa del datagrama de IP. IPsec comprende la base para la interoperabilidad de "tuberías" aseguradas de terminal-a-terminal, túneles encapsulados y Redes Privadas Virtuales (VPNs). IPsec esta basado en el algoritmo Diffie-Hellman y el algoritmo RSA para el intercambio de llaves. Para la encripción simétrica, los algoritmos DES y Triple DES son utilizados. En situaciones donde mayor seguridad es requerida para encripción en IPsec, el algoritmo RC5 es utilizado comúnmente. Las capacidades de IP son aplicadas en la capa de IP y para otorgar sus servicios de seguridad utiliza los protocolos del ***encapsulating security payload*** y ***authentication header***. Se recomienda el uso de este protocolo si se esta utilizando la versión 4 del protocolo de Internet.
- **SSL**. Secure Socket Layer (SSL) provee una capa de seguridad entre TCP y las capas de protocolos de aplicación. SSL otorga integridad y confidencialidad para cualquier flujo de datos TCP y puede ser usado con otros protocolos de nivel aplicación como http, Telnet, etc. Después de habérsele hechos algunos cambios a SSL 3, se obtuvo TLS (Transport Layer Security). Los algoritmos que utiliza se pueden seleccionar de varios disponibles. Este protocolo puede utilizarse tanto en computadoras clientes como en servidores y se recomienda en gran medida su utilización cuando se quieran hacer transacciones con tarjetas de crédito o establecer conexiones aseguradas por Internet.

JAVA. Sun Microsystems desarrolló el concepto de ***applet***, un programa que corre dentro de un navegador de Internet. Este tipo de programas son descargados de la red de manera dinámica con la finalidad de que los navegadores puedan entender e interpretar nuevos tipos de información que aparecen en las páginas web. Tal extensibilidad le permite a los navegadores crecer y adaptarse a las nuevas necesidades, la descarga de código sin la participación directa o conocimiento tiene serias implicaciones de seguridad. Sun Microsystems diseño el subsistema Java para encarar los problemas de seguridad. Java consiste de un interprete para una maquina virtual, la cual es independiente del tipo de máquina por lo que un solo ***applet*** puede usarse con cualquier computadora. Java esta diseñado para encargarse de los problemas de seguridad protegiendo al navegador y al usuario de ataques. Sin embargo en sus primeras versiones pueden causarse negación de servicio, degradación de servicio, encubrimiento de comunicaciones y modificaciones en el navegador. Java presenta las siguientes vulnerabilidades: ausencia de una política de seguridad bien definida, falta de un mecanismo de seguridad que sea siempre invocado, falta de un mecanismo de seguridad que sea a prueba de entradas, falta de defensa profunda, falta de una base confiable de computo. Sin embargo en nuevas versiones del mecanismo Java se han arreglado varios de estos problemas de seguridad, al mismo tiempo que varios navegadores funcionan de manera mas suave y ya consideran entre sus actualizaciones de seguridad la descarga de ***applets***. En caso de utilizar una versión vieja de los navegadores con Java se recomienda actualizarla a las ultimas, y estar continuamente descargando parches de seguridad para los navegadores que se encuentran disponibles en Internet.

COPIAS DE RESPALDO. Para cualquier sistema operativo que este usando la terminal, es recomendable un mantenimiento periódico de todas las copias de respaldo del sistema, las cuales serán útiles en la reinstalación del sistema en caso de que algún ataque informático cause daños irreparables en el sistema o por efecto de virus que borren archivos clave. Con estas copias de respaldo también se deben tomar ciertas precauciones de seguridad, por ejemplo, los respaldos deben guardarse de preferencia fuera de la terminal pero que estén fácilmente disponibles para emergencias; estas copias de respaldo pueden ser encriptadas para mayor protección, sin embargo, hay que asegurarse de tener acceso rapido a los programas de desencripción.

DETECTORES DE INTRUSOS. Otro grupo de herramientas de mucha utilidad para la seguridad de esta configuración son los detectores de intrusos. Los detectores de intrusos se aplican como complemento a los *firewalls* ya que estos no pueden detener a un atacante o pirata si enmascara el tráfico hacia dentro de la protección o si tiene comunicación directa con alguna aplicación.

Los detectores de intrusos se clasifican de dos maneras: sistemas de detección de intrusos en redes (NIDS) y sistemas de detección de intrusos en anfitrión (HIDS), así que para la segunda configuración de sistemas mostrada en este documento, será útil la capacidad para host individuales. El área de la detección de intrusos se encarga de informar de los eventos que puedan ser considerados como parte de un intento de intrusión en el sistema. Un efectivo sistema de detección de intrusos (IDS) debe ser capaz de diferenciar entre un acceso permitido por alguna aplicación que pone en marcha otros programas y uno no autorizado que busca vulnerar, robar o dejar inhabilitado ciertos recursos. El sistema de detección de intrusos también debe proporcionar conocimiento al administrador del sistema o responsable de la seguridad sobre la puesta en marcha de un ataque antes de que tenga éxito.

Generalmente la técnica para detectar intrusiones es el análisis por reconocimiento de patrones de ataques conocidos. En este aspecto son parecidos a los detectores de virus, ya que buscan detectar patrones para diferenciar un ataque de algo que no lo es. Para esto se basan en la búsqueda de anomalías, para llegar a ellas se emplean las técnicas de: clasificacion, episodios frecuentes, asociación de valores y análisis adaptivos. Para un desempeño eficaz se debe instalar primero el detector en modo de "aprendizaje" para analizar la información que recibe con un funcionamiento normal, posteriormente se dispone el detector en modo "analizar" para que este pendiente y busque actividad irregular, por ejemplo: el trafico fuera de horas de oficina, acceso repetitivo a algún recurso, etc. Sin embargo se debe mencionar que no son técnicas sin fallas, se pueden presentar **falsos positivos** los cuales son alarmas de intrusiones cuando no existe tal, los **falsos negativos** son intrusiones que pasan desapercibidas. Los HIDS tienen la ventaja de que normalmente presentan un menor número de falsos positivos que los sistemas NIDS. Además de la posibilidad de otros problemas inherentes a los detectores, en donde cada paquete que entra al sistema debe ser analizado, decodificado y su contenido revisado, lo cual representa una enorme carga de trabajo para el sistema. Afortunadamente con el paso del tiempo los detectores han mejorado y ahora podemos encontrar que tienen la capacidad de trabajar en redes de transito elevado con velocidades de Gigabit e inmunidad a las técnicas *stealth* que utilizan los piratas. Algunos ejemplos de herramientas de detección son: ***Omniguard, Cisco Secure IDS, RealSecure, Kane Security Analyst, Centras.***

Los IDS deben adaptarse a los recursos de la empresa o lugar donde se tenga el sistema que se quiere proteger y estos deben ser incluidos en las políticas de seguridad de la empresa.

CONTROL DE ACCESO Y AUTENTICACIÓN. Para un sistema que consta de una computadora con conexión a Internet donde queremos tener información segura, podemos seguir las siguientes recomendaciones en cuanto a la instauración de un programa que controle los accesos a una terminal:

- La implementación de bitácoras de acceso a la computadora en conjunto con un proceso de autenticación de usuario por medio de passwords, así, en la bitácora quedara asentado quien tuvo acceso a la terminal, el día y la hora y las operaciones que llevo a cabo en ella.

- Dentro de los programas de acceso se puede implementar la característica de que los usuarios solo podrán acceder la terminal a cierta hora del día, teniendo un control total sobre quien esta usando a la maquina a determinada hora.

El control de acceso considerara el proceso de autenticación de usuarios por medio de medidas de software, es decir, por medio del uso de passwords. La autenticación de los usuarios debe considerar varias situaciones: usuarios que escriban mal su passwords, malfuncionamiento del teclado, etc. Para el caso de uso de passwords ciertas medidas pueden ser programadas por dentro del programa controlador de accesos:

- Implementar un pequeño retardo en el proceso de verificación de 5 a 10 segundos. Para un usuario normal este proceso presentara una molestia mínima, sin embargo, para un posible perpetrador de robo de información y acceso no autorizado que use programas de ataque por búsqueda en diccionario, este retardo en cada intento de introducción de password hará que el ataque sea infeasible.
- Determinar el número de intentos de passwords equivocados que puede hacer un usuario. En caso de que sea muy importante para el negocio mantener ladrones fuera del sistema, con tres oportunidades basta. Si se dan las tres entradas equivocadas la cuenta del usuario debe ser dada de baja y solo el encargado de seguridad puede volverla a habilitar. Esto facilita la identificación de cuentas que están bajo ataque o en peligro por perpetradores.
- Programar el sistema para que obligue a los usuarios a cambiar de password periódicamente. Para evitar el reuso de passwords algunos sistemas de control de acceso rechazan cualquier password que haya sido usada recientemente.

Una técnica muy recomendable en el uso de passwords es utilizar los llamados passwords de "uso único" (*one-time password*). Estos cambian cada vez que son usadas. En los passwords de uso único al usuario se le asigna no una frase, sino una función matemática. Aquí el sistema da un argumento para la función y el usuario debe introducir el valor resultante. Un sistema que utilice esta técnica es llamado desafío-respuesta (*challenge-response*) porque el sistema le presenta al usuario un desafío y determina la autenticidad del usuario por su respuesta. Las funciones que se definen para los password de uso único pueden llegar a ser muy complejas, por ejemplo: $f(E(x))=E(D(E(x))+1)$ en donde la computadora envía un valor encriptado $E(x)$ y el usuario debe desencriptar el valor, aplicar la función aritmética $+1$ y encriptar el nuevo resultado para enviarlo de regreso al sistema. Los passwords de uso único son muy seguros, ya que si uno es descubierto no es de utilidad.

Estas recomendaciones son hechas pensando en que solo se debe desconfiar del usuario, pero existe el caso en que el sistema ya haya sido comprometido porque es muy sencillo crear un programa que muestre o simule el símbolo del sistema y los espacios para el ID del usuario y el password, capture la información escrita y la guarde. En este tipo de ataque el perpetrador escribe el programa, lo coloca en la terminal, espera que alguien escriba su password y se aleja sin que nadie se de cuenta. Las recomendaciones para evitar este tipo de ataque son:

- Asegurarse de siempre reiniciar la ruta del sistema. En algunos sistemas el presionar la tecla BREAK detiene los procesos que se realizan, o proceder al apagado y encendido de la terminal.
- Para asegurarse que la computadora esta corriendo el sistema que se desea, podemos programar el control de acceso para que antes de introducir password o datos confidenciales, muestre la fecha de la ultima vez que el usuario entró al sistema. Si se desea un mayor nivel de seguridad se puede encriptar el mensaje con la fecha, y el usuario se encargara de desencriptar y verificar la información, si es correcta el usuario encripta la fecha y el password para garantizar que un intruso no haya interceptado el password. Estas encripciones y desencripciones pueden ser hechas con algoritmos del tipo DES.

Varias compañías de software se dedican a desarrollar sistemas de control de acceso. Estos paquetes proveen de autenticación de usuario, limitación en los accesos y bitácora de registro, por ello es recomendable la utilización de estos programas.

CONTROLES DE HARDWARE

BIOS. En esta configuración también se puede aplicar el método de seguridad del BIOS. El BIOS contiene los datos de configuración y de información del sistema y al mismo tiempo varios parámetros cambiables. El orden de los dispositivos de arranque, que es controlado por el BIOS, es causa de preocupación porque casi todos los sistemas operativos tratan de arrancar primero desde la unidad de discos, después desde la unidad de CD o del disco duro, alguien podría aprovecharlo y reiniciar el sistema desde un disco que contiene código ejecutable para crear puertas traseras que pueden ser explotadas por Internet. Para la eliminación de esta vulnerabilidad, hay que configurar el BIOS para que arranque desde el disco duro desde la primera vez, y si es posible, eliminar la unidad de disco y el CD-ROM de la secuencia. Posteriormente agregar un password al BIOS, obligando a que se introduzca un password para permitir hacer cambios al BIOS y evita que alguien vuelva a cambiar la secuencia de arranque para usar la unidad de disco, esto protege también de alguien que quiera evitar el inicio del sistema. Sin embargo, sigue siendo muy sencillo evadir la protección de password en el BIOS. Solo se debe cambiar la posición de un jumper en el motherboard y así la configuración del BIOS volverá a su estado por default deshaciéndose del password. La protección del BIOS depende de los conocimientos que tenga el atacante en cuanto a mover el jumper, ya que hay que abrir la computadora y localizar el jumper. Esto afecta a todos los sistemas operativos ya que el BIOS es parte de la arquitectura de la PC.

Si se utiliza el sistema LINUX, existe la opción de utilizar el Linux Loader (LILO), esté se coloca en el registro del *master boot* del sistema. BIOS le cede la ejecución a LILO. LILO cargara el *kernel* de LINUX, y este completara el proceso de arranque. LILO permite que se arranque el sistema en un cierto estado de operación ***init.*** Cuando un usuario desea arrancar en el estado 1 (***init state 1***) el requisito de la autenticación es pasado por alto, y se presenta la línea de comandos de la consola con privilegios de raíz. Para poder evitar este problema, se puede agregar un password a la configuración de LILO, la cual se encuentra en el archivo ***/etc/lilo.con***. De esta manera será necesario introducir un password cada que se desee arrancar un sistema operativo, o incluso usar un password distinto para cada sistema operativo disponible. Para prevenir que los usuarios vean la información del archivo, se configuran los permisos para que solo se puedan leer desde raíz. No hay información acerca de que algún otro sistema operativo otorgue la posibilidad de asegurar la información del BIOS.

SMARTCARD. Otra opción que se puede usar de manera conjunta para protección de la computadora es la smartcard, la cual genera cada determinado tiempo un password que permite el acceso hacia las áreas de la información critica que contiene la PC. Si no se tiene el password o la smartcard, el acceso es prácticamente imposible ya que el password que genera esta formado por letras y números de distinta longitud, obligando a un ataque largo y tedioso con programas de fuerza bruta. Con esto se logra tener un nivel mayor de seguridad porque el uso de smartcard no puede ser violada con el simple cambio de un jumper. Muchos negocios utilizan técnicas de autenticación biométrica en conjunto con smartcards; las técnicas biométricas miden alguna característica física única del usuario, tal como el patrón de la voz, de cara, el orden de los vasos sanguíneos de la cornea y las huellas digitales. Tradicionalmente, las representaciones digitales de las características biométricas ocupan un espacio entre 100 y 600 bytes y por ello se pueden acomodar en una smartcard. Los pasos característicos de una autenticación de usuario por medio de smartcard y medidas biométricas son los siguientes:

1. Insertar la smartcard en el lector, esta contiene las llaves criptográficas y los datos correspondientes a la huella digital del usuario.
2. Se introduce el número de identificación privada (PIN), así, se libera la representación electrónica de la huella digital.
3. Ahora se coloca el dedo en el escáner, esta huella es comparada con la guardada en la smartcard.

4. Si la comparación es positiva, los datos de la huella en la smartcard son convertidos a un valor numérico y se combinan con el PIN de la smartcard para formar una llave de encripción simétrica la cual desencripta la llave privada.
5. Un número aleatorio es generado por la computadora donde se conecta la smartcard, este número es transferido a la smartcard.
6. La llave privada en la smartcard es usada para encriptar el número aleatorio y mandarlo de vuelta a la computadora.
7. La computadora verifica que una llave pública certificada obtenida de algún directorio en red desencripte el número aleatorio y verifica que este sea el mismo que se envió originalmente a la smartcard.
   Este proceso se encarga de autentificar de manera irrefutable al usuario de la smartcard.

MODEM. Uno de los dispositivos más comunes en un sistema donde solo se tiene una computadora con conexión a Internet es el MODEM. El MODEM permite a una computadora acceder a Internet por medio de una línea telefónica y por ello se deben tener ciertos cuidados para que no sea un camino de entrada a piratas, gusanos, o virus. Existen algunos MODEMs que tienen instalaciones de seguridad interna que proveen de métodos de acceso y autorización por password y soportan el acceso remoto a múltiples ambientes de protocolos. Si no se requiere un nivel muy alto de seguridad se puede conseguir un sistema de administración de MODEM, el cual provee números específicos para los puertos de marcación, además de cuentas de usuarios para protocolos específicos o para la terminal de acceso. Otros sistemas de acceso seguro por MODEM permiten la emulación de instalaciones terminales y tienen capacidades de protocolo de acceso remoto, rastreo de sesión, monitoreo en tiempo real, métodos de autenticación de usuario, alarmas, rastreo de perfil de usuario, menú de usuario y otorga instalaciones de acceso a hardware. Este ultimo es un MODEM bastante completo en cuanto a seguridad.

PUERTOS INFRARROJOS. En esta segunda configuración de sistemas también se aplica la seguridad para el puerto infrarrojo. Muchas de las computadoras portátiles vienen equipadas con estos puertos. Los puertos IR son vulnerables a intentos de acceso, robo de información o causar un sobreflujo del buffer y la aparición de la pantalla azul y reinicio del sistema. Para evitar esto se pueden tomar las siguientes medidas:

- Descargar los parches y actualizaciones que cubran esta vulnerabilidad y que ya están disponibles
- Hay que deshabilitar los dispositivos infrarrojos si no están en uso, no basta con deshabilitar la comunicación, sino que hay que deshabilitar todo el dispositivo utilizando el programa Administrador de Dispositivos
- Asegurarse que los puertos infrarrojos tienen bloqueada la línea de vista

También se puede colocar cinta opaca sobre el puerto aunque esto solo servirá si el oponente no tiene acceso a la máquina.

POLÍTICAS

Para la configuración dos de sistemas informáticos también deben definirse ciertas políticas de seguridad, ya que los riesgos aumentan al tener la computadora conectada a Internet. Es conveniente que antes de enunciar políticas dentro del negocio o compañía se definan los lineamientos de uso, hacer un análisis de riesgos en el sistema y establecer una estructura para el equipo de seguridad. Los lineamientos de políticas deben encargarse de contestar las preguntas: ¿A QUIEN se le permite acceso? ¿A QUE recursos? y ¿COMO se regula el acceso?. Las políticas también deben especificar: las metas en seguridad de la organización, quien tiene la responsabilidad de la seguridad, y el compromiso de la organización con la seguridad. En esta configuración se tiene una computadora con conexión Internet, se pueden imponer las siguientes políticas, aunque esto depende de las necesidades de seguridad del negocio ya que las políticas se pueden hacer más restrictivas o más libres.

- Cada determinado tiempo cambiar de passwords para conexión a Internet.

- Los usuarios no deben utilizar el nombre propio o apellido como clave de acceso, ni el nombre de la pareja, hijo o mascota.
- Los usuarios del sistema no deben abrir correos electrónicos provenientes de desconocidos.
- El encargado de la seguridad del sistema debe aplicar auditorias con los programas correspondientes para estar al día en cuanto a vulnerabilidades.
- Los usuarios del sistema no deben escribir los passwords en ninguna lista o papel.
- Los usuarios deben tratar de utilizar distintos passwords para cada aplicación, inicio del sistema, o conexión a Internet.
- El encargado de la seguridad del sistema debe buscar en Internet los parches necesarios para la corrección de vulnerabilidades que existen en el sistema operativo que se este utilizando en la computadora.
- Instruir a los usuarios para que no revelen a gente no autorizada las claves de acceso.
- Nunca entrar a Internet si no esta activo el *firewall*, el programa antivirus, o el programa encargado de detectar intrusos en el sistema.
- La firma de cláusulas explicitas dentro de los contratos de los trabajadores en donde acepten el no revelar información a competidores. Así se podrá emprender acción legal si esto se llega a presentar.

Las políticas de seguridad son reglas que nos dictan como conservar la seguridad y las acciones a tomar en caso de una ruptura a la seguridad e incursión dentro de la maquina que queremos proteger.

CONTROLES FÍSICOS

AUTENTICACIÓN BIOMÉTRICA. Para la configuración dos de los sistemas informáticos se toman en cuenta las técnicas biométricas para el control de acceso a la computadora. Se pueden emplear los siguientes métodos de protección:

- Revisión de retina
- Las técnicas de reconocimiento de voz y de firma de usuario, aunque no son biométricas
- Técnicas de autenticación de rostro, mano o huellas digitales

Previo a la implementación de alguna de estas técnicas debemos evaluar los siguientes factores dentro de la organización: nivel de seguridad que se necesite, costo y tiempo de implementación, aceptación de los usuarios y confiabilidad.

- Nivel de seguridad. El reconocimiento de voz y de firma son técnicas aceptables cuando se habla de usos no relacionados con autorización de acceso a la PC, sin embargo son útiles para la autenticación de usuarios de PC. Las técnicas biométricas que identifican características físicas son más confiables y otorgan un nivel mayor de seguridad.
- Costo y tiempo de implementación. Cuando se desea implementar un sistema de autenticación biométrica de usuario, se debe de hacer en conjunto con el proveedor de computadoras y tomar en cuenta que hay que buscar e instalar el software y hardware compatible con la PC para autenticación (cámaras, lectores, *scanners*), el software necesario para mantener la base de datos de usuarios, el tiempo que se lleva integrar el hardware de autenticación en el ambiente de trabajo, el entrenamiento del *staff* para manejar el nuevo sistema, el entrenamiento de los usuarios con el nuevo protocolo de autenticación y la actualización continua de las bases de datos.
- Aceptación de usuarios. Los usuarios generalmente aceptan las técnicas que son menos intrusivas o gorrosas, tales como identificación de huellas, rostro o mano. Aquí es responsabilidad de la organización el entrenar a los empleados para que se familiaricen con los nuevos requerimientos antes de que el sistema sea implementado.
- Confiabilidad. La revisión de retina e identificación de iris son altamente eficientes para identificar individuos, sin embrago, son muy costosas y la mayor parte de los negocios no necesitan este nivel de confiabilidad. Técnicas de autenticación de huellas, mano, y rostro ofrecen buena confiabilidad y requieren una menor inversión en equipo de revisión. Los

cambios físicos tales como cortadas, cicatrices y el envejecimiento pueden afectar la identificación, sin embargo las bases de datos se pueden actualizar.

Existen dos términos que describen la funcionalidad de las técnicas biométricas: la razón de falsa aceptación (*False Aceptance Rate*, FAR) el cual describe la probabilidad de que un intruso sea aceptado con una medida que no le pertenece de un usuario enrolado. La razón de rechazo falso (*False Rejection Rate*, FRR) es la probabilidad con que un usuario enrolado sea rechazado. Se considera que un buen equipo biométrico tiene un bajo FRR y FAR. Casi siempre hay un intercambio entre seguridad y conveniencia, en los sistemas biométricos mientras más seguro el sistema (mas bajo FAR) es más inconveniente para el usuario, ya que ocurren más rechazos falsos. Similarmente, mientras más conveniente sea el sistema, menos seguridad tiene. Los sistemas biométricos le permiten al usuario elegir entre un amplio rango de niveles de FAR/FRR.

Tomando en cuenta que puede haber ocasiones extremas en donde se utilice un dedo cortado de la mano o dedos falsos, algunos proveedores miden el calor del dedo en el escáner, otros miden su conductividad para evitar casos donde se modifiquen las huellas con silicón. La solución más adecuada es por medio de la medición **espectroscópica** de la cantidad de hemoglobina oxigenada en la sangre, ya que es imposible de pasar con dedos artificiales y los resultados de esta prueba son muy distintos para dedos vivos y dedos cortados.

HERRAMIENTAS Y MEDIDAS FÍSICAS. En los controles físicos consideramos también las estrategias y herramientas que ayudan a impedir los incidentes de robo o perdida de equipo de computo. Reforzar el blanco (*target hardening*) es un proceso de edificar una serie de barreras físicas para desalentar el progreso de un adversario, con el reforzamiento se pretende que el atacante renuncie a la idea antes de atacar, se rinda durante el ataque o demorarlo lo suficiente para que una fuerza de respuesta se encargue del ataque antes de que sea completado. En esta configuración tenemos una computadora conectada a Internet, así que las medidas de seguridad son muy similares al caso donde solo tenemos una computadora sin conexión:

- Designar un oficial de seguridad departamental, quien reportara rupturas en la seguridad y actos ilegales. Además será el responsable de implementar, coordinar, mantener y monitorear un programa de seguridad departamental.
- Se debe restringir el acceso a lugares donde se encuentre el closet o gabinete que contiene cableado de conexión a Internet.
- Guardias deben organizar un patrullaje de seguridad en el área donde esta el acceso a la computadora resguardada, llevado a cabo por guardias.
- Establecer puntos de recepción en el edificio entre áreas funcionales o zonas seguras.
- Definir claramente los limites del acceso público dentro del edificio, por medio de señalamientos.
- Para proteger una computadora de escritorio, se puede colocar el monitor, teclado, impresora y CPU en un gabinete bajo llave. En caso de una laptop se puede utilizar un gabinete más pequeño.
- Instalar puertas y ventanas que den entrada al edificio u oficina donde esta la computadora a proteger que cuenten con alarmas contra apertura o ruptura.
- Los cables de aseguramiento de computadoras son muy populares hoy en día y pueden ser otra opción en lugar del gabinete, así como placas de acero para aseguramiento que mantienen la computadora junto a la mesa.
- Vigilar frecuentemente que no haya algún cable superpuesto al cable que permite la conexión a Internet de nuestra computadora.
- Para evitar el acceso a las unidades de disco de la computadora se emplean candados con llave.

Todas estas medidas son para prevenir el robo y destrucción, aunque se puede idear medidas más estrictas dependiendo de los requerimientos de la empresa.

NIVEL DE SEGURIDAD

En la configuración dos se tiene una computadora con conexión a Internet. Antes de aplicar las recomendaciones, el nivel de seguridad es apenas de **1** si el sistema cumple con protección antivirus y protecciones contra robo físico.

Su operatividad esta dada por la formula:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{1} = 1$$

Con las recomendaciones hechas en los apartados de **encripción, Controles de Software, Controles de Hardware, Políticas** y **Controles Físicos** se cubren las características descritas para la obtención del nivel **5** de seguridad.

Su nivel de operatividad esta determinado por la formula:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{5} = 0.2$$

El nivel de operatividad es el más bajo, obviamente esto depende de las necesidades en seguridad de la empresa o negocio. Si se desea un mayor nivel de operatividad, hay que buscar que servicios de seguridad no son necesarios para la operación del sistema que se tiene y descartarlos.

Tabla 4.3 - Niveles de Seguridad y Operatividad

Nivel de seguridad por default	**1**
Nivel de Operatividad por default	**1**
Nivel de Seguridad con recomendaciones	**5**
Nivel de Operatividad con recomendaciones	**0.2**

Utilizando las definiciones de seguridad de los niveles en el Orange Book de la página 22. Si se quiere saber en que nivel queda el sistema descrito en la configuración dos después de aplicar las recomendaciones y con una correcta implementación de las políticas, control de accesos y autenticación, sería aproximadamente el nivel **B3**. El cubrir las características del nivel B2 depende de la etiquetacion de objetos y eso puede variar en diferentes sistemas por la información y recursos que se manejen, así que bien puede ser cubierto y bien puede no serlo, depende del administrador. Así, el sistema muestra un nivel de seguridad muy elevado, solo por abajo del nivel A, suficientemente seguro para que diferentes usuarios trabajen en él, sin haber fuga de información.

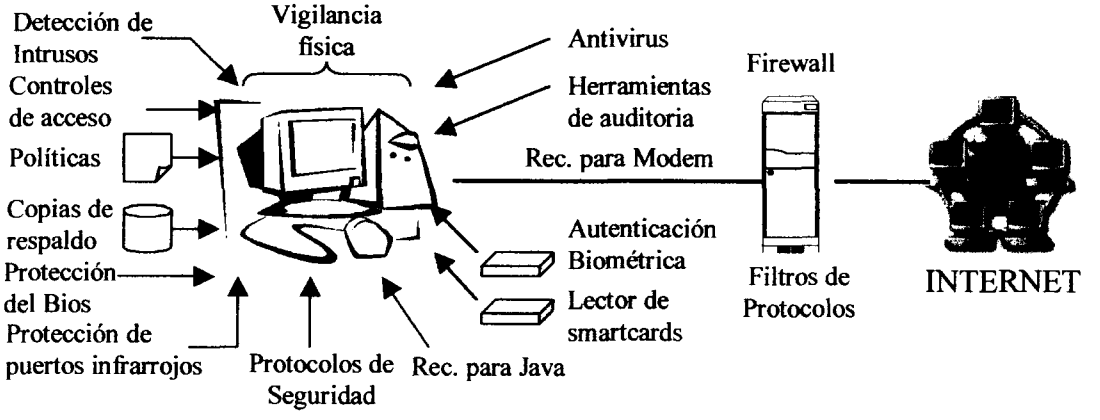


Figura 4.5 - Configuración dos protegida

CONFIGURACIÓN 3 - Una red local sin conexión a Internet.

Una configuración que tiene muchas aplicaciones en distintos negocios es una red de computadoras interna, pero sin ninguna conexión a Internet. Para lograr tener la confianza de que en este sistema no se efectuara una operación indebida, y que el funcionamiento de las distintas aplicaciones y bases de datos compartidas por la red local será eficiente, se deben instaurar ciertas medidas en software y hardware. Las características por default de seguridad de una red de computadoras sin conexión a Internet consisten en: No contar con un administrador de red o responsable de seguridad, sistemas operativos sin parches de seguridad instalados, ningún tipo de autenticación de usuario o codificación para proteger archivos importantes o acceso a la red, servicios de red disponibles para personal no autorizado, ningún software de auditorias, tampoco detectores de intrusos, además de tener casi todas las características de seguridad para operación en red de los sistemas operativos al mínimo por default. Muchos de los equipos de computo vienen de fabrica con programas antivirus instalados (aunque no necesariamente actualizados) y candados o elementos de seguridad física para cada computadora, al tener una red puede ser que todas las computadoras estén en un solo lugar y se asegure el cuarto con llave.

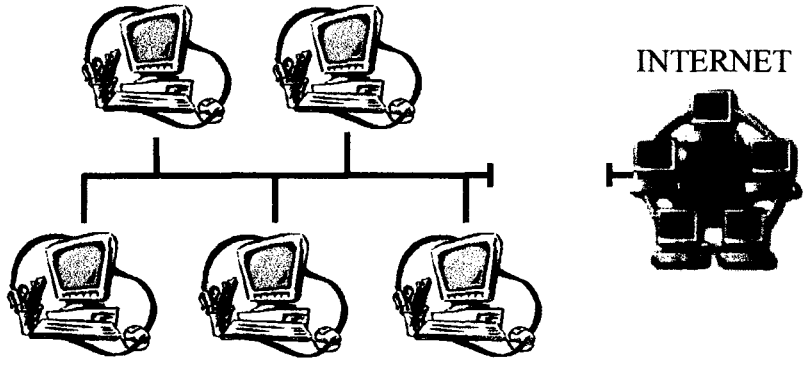


Figura 4.6 - Una red sin conexión a Internet.

En general, para una configuración de este tipo se recomienda instituir una serie de medidas preventivas de seguridad, ya que aun y cuando nuestro sistema no esta en riesgo de caer victima de piratas a través de Internet, existe la posibilidad de que nuestro sistema caiga victima de empleados y usuarios con poca honestidad. Enseguida se explican a detalle las recomendaciones y sugerencias para mantener segura una red local sin conexión a la red mundial.

ENCRIPCIÓN

La encripción es una herramienta muy útil con la cual podemos proveer de privacía, autenticidad, integridad y acceso limitado a los datos. Debido a los muchos riesgos existentes, es normal que se opte por asegurar la información en las redes encriptandola y en combinación con los otros controles. En las aplicaciones de red, la encripción puede ser implementada entre dos terminales o entre dos aplicaciones. El problema con la encripción es el uso de llaves, ya que estas deben ser enviadas a la fuente y receptor de los mensajes.

En la encripción de enlaces (*link encryption*), la información es encriptada justo antes de que el sistema la coloque en el enlace de comunicaciones. En este caso la encripción se lleva a cabo en las capas 1 y 2 del modelo OSI. La desencripción ocurre justo cuando la información entra en la computadora receptora. En este método la encripción protege el mensaje en transito entre dos computadoras, sin embargo, el mensaje esta en texto simple dentro del anfitrión y en las capas superiores a la 1 dentro de la terminal fuente y la receptora. Incluso si el mensaje tiene que pasar por algún *host* también podrá verlo de manera simple y no encriptado ya que las tablas de ruteo y direccionamiento no se leen en la capa física, sino en las de enlace y de red. Esto puede

crear un problema de seguridad si el *host* no es confiable o su seguridad ha sido comprometida. La encripción de enlace es invisible al usuario y es llevada a cabo por un protocolo de capa de red de bajo nivel. En un mensaje encriptado de esta manera los encabezados (*header*) y la información de control son agregados por el lado del origen y removidos en el lado del receptor. Como la encripción se lleva a cabo en la capa mas baja, no solo el mensaje es encriptado, sino los headers de transporte, red y sesión. El uso de este método se recomienda si los riesgos de seguridad son mayores en las líneas de comunicación.

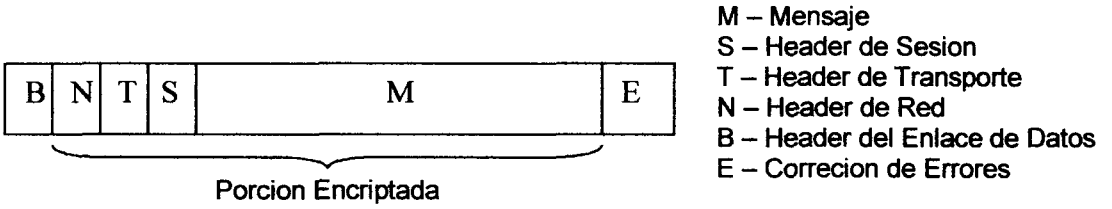


Figura 4.7 - Mensaje con encripción de enlace

Otra forma de proporcionar seguridad a una red por medio de la encripción es con el método de terminal a terminal (*End-to-End Encryption*). Este provee encripción por un dispositivo de hardware entre el usuario y el *host*. Una alternativa para esto, es la encripción realizada por software en la propia computadora. De cualquier manera, la encripción se realiza en las capas 7 o 6 del modelo OSI y por ello solo se encripta el mensaje y no sus encabezados (*headers*). La encripción asegura que el mensaje este encriptado para cualquier capa, así, si el mensaje es interceptado en su transcurso hacia otro punto seguirá estando encriptado.

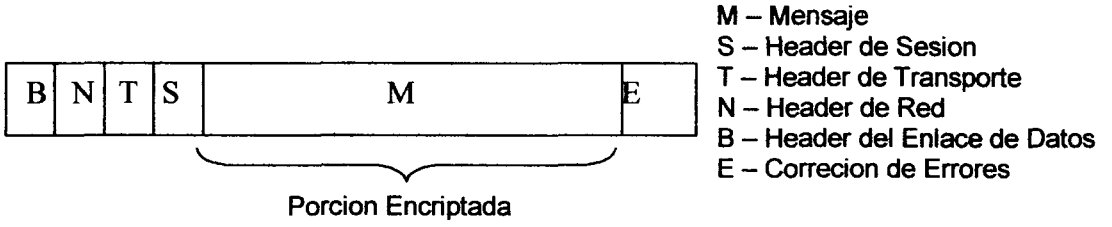


Figura 4.8 - Mensaje con encripción de terminal a terminal

La encripción de enlace es más rápida, más fácil para el usuario y utiliza pocas llaves, ya que solo requiere una por cada par de terminales. La encripción de terminal a terminal es más flexible, puede ser usada de manera selectiva y al ser hecha a nivel usuario se puede llevar a cabo dentro de la aplicación.

Cada red tiene necesidades distintas y por ello ninguna forma es completamente eficaz para todo tipo de redes. Si los recursos lo permiten y existe el caso en que no confíe en los otros *host* dentro de la red se pueden utilizar los dos tipos de encripción. Sí la encripción de datos no es muy tardada, entonces las molestias y rendimiento negativo sera poco.

Otro de los casos donde la encripción es de utilidad es para codificar la información critica almacenada en discos, CD, archivos en disco duro, etc. Para este almacenamiento se puede optar por encripción simétrica, sí solo una persona esta a cargo de su almacenamiento, encripción y desencripción.

CONTROLES DE SOFTWARE

Una red de computadoras como su nombre lo indica consiste de varias máquinas interconectadas. Cada una de estas máquinas contiene un sistema operativo y software instalado.

En la configuración tres no hay presente la conexión a Internet, por ello no existe el peligro de intrusiones externas, sin embargo las vulnerabilidades son numerosas y para controlarlas se pueden aplicar las medidas que se describen a continuación.

PROGRAMAS AUDITORES. Una de las opciones para la protección de una red de computadoras es la utilización de programas para la seguridad de la información, tales como software para la administración de eventos de seguridad, para el escaneo de vulnerabilidades en el sistema o proveedor de servicios de seguridad. El software para la administración de la seguridad de una manera centralizada se esta volviendo la forma más popular entre los administradores de red para estandarizar y analizar la información concerniente a eventos de seguridad en una sola consola central. Los programas auditores se encargan de revisar la condición y administración de los puntos de seguridad de la red. En la configuración tres de sistemas, los programas auditores nos darán la siguiente información del sistema:

- Las vulnerabilidades que tiene la red, de actualizaciones recomendables para los distintos programas que contiene nuestro equipo. Ya que cualquiera de ellos puede representar un problema de seguridad.
- El flujo de datos a través de los dispositivos de seguridad instalados en las computadoras y en la red y los reportes de los controles de seguridad.
- La información de los programas auditores debe incluir informes sobre cualquier usuario o entidad en la red que trate de obtener un nivel de seguridad mas elevado, información sobre accesos y salidas del sistema, accesos de superusuario, y cualquier otro cambio de acceso o estatus.
- Una medición de la eficiencia en las operaciones, por ejemplo, cuantos virus fueron detectados vs cuantos fueron limpiados.
- Una evaluación del apego a las políticas de seguridad o estándares, por ejemplo, los estándares en antivirus especifican que todos los archivos ***.DAT***, donde se mantiene la información de nuevos virus, deben ser actualizados cada cierto tiempo.
- Establecimiento de las bases para un plan comprensivo de respuesta a incidentes de seguridad.

El tipo de información recopilada es distinta para cada sitio y configuración, estando limitada la recopilación solo por el espacio disponible para su almacenamiento. La información generada por los programas auditores puede almacenarse de varias formas: en archivos de lectura y escritura dentro de la terminal de monitoreo central, en un dispositivo donde se escribe una vez y se puede leer varias (CD-ROM), o en un dispositivo de solo escritura (impresora de línea). Cada una de estos métodos tiene sus ventajas y desventajas. Si se opta por grabar los registros en un archivo de lectura-escritura dentro de la terminal central se tendrá acceso instantáneo a los registros para su análisis en el momento de un ataque, por otro lado, es poco confiable ya que, alguien logra acceder a este sistema por algún método y su intención es robar información, modificarla, o falsificarla, puede fácilmente borrar cualquier dato de la intrusión al manipular los archivos del registro. La segunda opción es guardar la información en un medio donde se escriba una vez, como un CD; esto es un poco más complicado de configurar, la información no estara disponible instantáneamente y el costo es más elevado, aunque es un método mas seguro ya que, un intruso no podrá modificar los archivos en un CD para cubrir su intrusión. La tercera opción para el almacenamiento de la información de auditoria es con un dispositivo de solo escritura, una impresora de línea quedaría en esta categoría; este método es de mucha utilidad si se requieren registros permanentes e inmediatos para el caso donde se quiere saber el punto exacto de una falla o ataque al sistema; si se quiere usar una impresora laser o algún otro dispositivo que ponga la información en espera se puede perder la información en el momento critico; las desventajas de este método son el mantener alimentada con papel la impresora y donde guardar todo el papel utilizado para un análisis posterior. La información de los programas auditores puede ser clave para la investigación, detención y proceso legal de los responsables de robo informático. Algunos ejemplos de programas que sirven para hacer auditorias de seguridad son: ***LT Auditor+ Version 8.0, Nessus, Nmap***.

PROGRAMAS ANTIVIRUS. Para una red de computadoras existe el riesgo de que si una de las maquinas es infectada por un virus toda la red puede ser victima, los virus informáticos están presentes y pueden llegar de manera accidental o intencional a la red, ya sea por medio de un archivo enviado de una terminal a otra, al compartir una aplicación infectada o por medio de un disco contaminado. El software antivirus debe ser instalado en cada una de las máquinas de la red si estas cuentan con disco duro. Enseguida se presentan recomendaciones de seguridad para tratar con la amenaza de los virus:

- Utilizar solamente software adquirido de vendedores confiables y bien establecidos.
- En caso de que se deba usar software proveniente de fuentes de calidad y honradez desconocidas, se recomienda probar este nuevo software en una computadora separada de la red, que no contenga disco duro ni disco de arranque. Se debe observar el comportamiento del software y buscar cualquier falla e indicios de actividad inexplicable en pantalla. Posteriormente hay que revisar la computadora de prueba con un programa detector de virus, diversos programas antivirus permiten crear un disco de detección.
- Crear un disco de arranque y mantenerlo seguro. Es necesario mantener este disco contra escritura durante el reinicio del sistema. El disco debe de prepararse antes de que el sistema se infecte y tenerlo a la mano en cuanto surja la necesidad.
- Crear y conservar copias de respaldo de los archivos ejecutables del sistema. Así, en caso de una infección, los archivos afectados pueden ser removidos y reinstalados de las copias limpias.
- Utilizar detectores (*scanners*) de virus regularmente. Muchos de los detectores disponibles hoy en día permiten la detección y la eliminación de los virus. Se recomienda tener mas de un detector porque uno puede encontrar virus que otros ignoran.

Las amenazas por virus informáticos no infectan un solo tipo de computadora o sistema operativo. Las PC son las más populares y por ello las que más sufren por virus, pero eso no significa que los propietarios de estaciones de trabajo de UNIX, LINUX, Macintosh estén exentos a estos riesgos. Los virus representan amenazas para cualquier programa almacenado sin protección contra escritura. Si las terminales de la red utilizan disco duro y sistema operativo se pueden aplicar las opciones de proteger los archivos contra escritura designándolos como "oculto" o "solo lectura", sin embargo, este tipo de protección puede ser superada por los programadores de virus fácilmente. No debemos de sentir que nuestros archivos de información, listas, hojas de trabajo, etc. están a salvo de ser infectados, los virus no solo se limitan a infectar los archivos de programa sino también afectan a los archivos de datos, esto lo logran al agregar a archivos de texto o de hojas de calculo ciertos comandos de inicio y así esparcen la infección o causan estragos. Si el sistema ha sido infectado hay ocasiones en que un simple apagado general y encendido de la maquina libra del problema ya que ciertos virus residen en memoria y al ser una memoria dinámica se pierde su contenido al quitar la energía, aunque se debe tener en cuenta que este método no funcionara si el virus esta guardado en disco o si se encuentra ya en el sector de arranque. Se deben tener muchos cuidados para mantener un sistema funcional y al mismo tiempo protegido de los virus.

PROTOCOLOS Y SISTEMAS DE ARCHIVOS. En esta configuración no hay conexión a Internet, lo que significa que no se utilizan los protocolos y sistemas de archivos que permiten la comunicación a través de ella. Sin embargo sí se consideran los protocolos para la transferencia en redes por lo que se agregan recomendaciones de seguridad al usar los protocolos o sistemas de transferencia de archivos en redes.

- **LPD**. El daemon para impresora de línea (*Line Printer Daemon*) permite que computadoras en red tengan acceso a los servicios de impresión en otra computadora. En un ambiente de red de área local LPD no tiene ningún problema de seguridad, pero puede tener vulnerabilidades si se conecta la red a Internet.
- **NFS**. El sistema de archivos en red (*Network File Systems*) permite la compartición de disco duro entre computadoras. Esta característica es de utilidad para los casos en que las

terminales de la red no tienen disco duro y dependen de un servidor de discos para sus funciones de almacenamiento. En el servidor de NFS debe especificarse a que terminales se les enviara la información. NFS no debe exportar o permitir conexión de cualquier terminal fuera de la red o permitirle la conexión a Internet.

- **NIS**. Los servicios de información en red (*Network Information Services*) funcionan de manera parecida a una aplicación cliente-servidor donde el servidor provee de información de usuarios y computadoras en la red. El sistema NIS provee de un sistema de archivos con password central para redes de computadoras. Igual que los anteriores no presenta vulnerabilidades a menos que la red se conecte a Internet.
- **SMNP**. Protocolo de administración simple de redes (*Simple Network Management Protocol*). Este protocolo permite que un administrador de red maneje los recursos a través de un nodo remoto. No presenta vulnerabilidad si la red se mantiene fuera de Internet.
- **TFTP**. Protocolo de transferencia de archivos triviales (*Trivial File Transfer Protocol*). TFTP es utilizado para reiniciar una computadora desde otro punto en la red. TFTP opera en el puerto 69, una operación cotidiana sería que una computadora inicia una sesión TFTP con un servidor de arranque desde donde transfiere los archivos de sistema necesarios para arrancar. Este protocolo también puede usarse para transferir archivos a cualquier computadora en la red, su uso más común es transferir software para configuración para sistemas sin disco duro, tal como ruteadores. Este servicio debe instalarse en una computadora o servidor que no tenga contacto con Internet o redes externas.
- **Windows X11**. Xwindows es un ambiente grafico para el software de aplicación de usuario. Este ambiente soporta servicios distribuidos usando puertos TCP y esta diseñado para controlar y mostrar de manera remota procesos a través de la red. En este sistema existe el riesgo de que un proceso dañino tome control o vigile la pantalla, el teclado y mouse. La necesidad de abrir muchos puertos le da a un intruso la oportunidad para usar un puerto abierto y comprometer un sistema confiable con una conexión vulnerable. Al usar este ambiente se recomienda usar un programa que vigile la detección de intrusos en la red, así como un antivirus con protección en tiempo real.

COPIAS DE RESPALDO. En las redes de computadoras deben hacerse copias de respaldo con frecuencia, debido a la gran cantidad de información que se maneja. Estas copias deben ser hechas de los archivos más importantes como las bases de datos que se comparten en la red y toda clase de archivos privados e importantes para el funcionamiento del sistema de cada computadora. Es recomendable un mantenimiento periódico de todas las copias de respaldo, las cuales serán útiles en la reinstalación del sistema en caso de que algún ataque informático cause daños irreparables en el sistema o por efecto de virus que borren archivos clave. Con estas copias de respaldo también se deben tomar ciertas precauciones de seguridad, por ejemplo, los respaldos deben guardarse de preferencia fuera de la red pero que estén fácilmente disponibles para emergencias; estas copias de respaldo deben ser hechas por el administrador del sistema o por el responsable de la seguridad en la red y para una mejor protección pueden ser encriptadas, sin embargo, hay que asegurarse de tener acceso rapido a los programas de desencripción.

DETECTORES DE INTRUSOS. Otro grupo de herramientas de mucha utilidad para la seguridad de esta configuración son los detectores de intrusos. Los detectores de intrusos se clasifican de dos maneras: sistemas de detección de intrusos en redes (NIDS) y sistemas de detección de intrusos en *host* (HIDS), así que para la tercera configuración de sistemas mostrada en este documento, sera útil la capacidad para proteger redes. El área de la detección de intrusos se encarga de informar de los eventos que puedan ser considerados como parte de un intento de intrusión en el sistema. Un efectivo sistema de detección de intrusos (IDS) debe ser capaz de diferenciar entre un acceso permitido por alguna aplicación que pone en marcha otros programas y uno no autorizado que busca vulnerar, robar o dejar inhabilitado ciertos recursos. El sistema de detección de intrusos también debe proporcionar conocimiento al administrador de red o responsable de la seguridad sobre la puesta en marcha de un ataque antes de que tenga éxito.

Generalmente la técnica para detectar intrusiones es el análisis por reconocimiento de patrones de ataques conocidos. En este aspecto son parecidos a los detectores de virus, ya que buscan detectar patrones para diferenciar un ataque de algo que no lo es. Para esto se basan en la búsqueda de anomalías, para llegar a ellas se emplean las técnicas de: clasificacion, episodios frecuentes, asociación de valores y análisis adaptivos. Para un desempeño eficaz se debe instalar primero el detector en modo de "aprendizaje" para analizar la información del transito y operaciones normales en la red y sus aplicaciones, posteriormente se dispone el detector en modo "analizar" para que este pendiente y busque actividad irregular, por ejemplo: el trafico fuera de horas de oficina, acceso repetitivo a algún recurso o aplicación, etc. Sin embargo se debe mencionar que no son técnicas sin fallas, se pueden presentar **falsos positivos** los cuales son alarmas de intrusiones cuando no existe tal, los **falsos negativos** son intrusiones que pasan desapercibidas. Los NIDS analizan todo el trafico de la red, examina los paquetes para buscar opciones no permitidas. El análisis en toda la red lo hacen mediante el uso de agentes sensores, los cuales reportan las alarmas hacia una consola central. La mayoría de los NIDS no necesitan software adicional en los servidores, sin embargo tienen la desventaja de un alto número de **falsos positivos** que con los reportes de los agentes incrementan el trafico en la red, y tienen dificultades para detectar ataques encriptados. Cada nueva versión de los detectores viene mejor preparada para las nuevas tecnologías y ahora podemos encontrar que tienen la capacidad de trabajar en redes de transito elevado con velocidades de Gigabit e inmunidad a las técnicas *stealth* que utilizan los piratas. Los detectores de intrusos pueden configurarse para que sean activos o pasivos. Si se designa como activo, el IDS responde ante una actividad ilegal de forma activa sacando al usuario de la red, si se designa como pasivo el programa detectara la actividad inusual, genera la alerta y un registro de ella.

Algunos ejemplos de herramientas de detección son: ***Omniguard, Cisco Secure IDS, RealSecure, Kane Security Analyst, Centras***. Los IDS deben adaptarse a los recursos de la empresa o lugar donde se tenga la red que se quiere proteger y estos deben ser incluidos en las políticas de seguridad de la empresa.

CONTROL DE ACCESO Y AUTENTICACIÓN. Una red de computadoras LAN permite compartir archivos, servicios de impresión, y el almacenamiento de archivos. En una red local se tienen aplicaciones corriendo en las terminales y al mismo tiempo enlazadas con otras, por ello el control de acceso es el responsable de la autenticación de los usuarios del sistema compartido por la red. Y en este caso el responsable de la implementación del control de acceso es el administrador del sistema. Las recomendaciones son muy parecidas a las de las configuraciones uno y dos:

- La implementación de bitácoras de acceso a la computadora en conjunto con un proceso de autenticación de usuario por medio de passwords, así, en la bitácora quedara asentado quien tuvo acceso a la terminal, el día y la hora y las operaciones que llevo a cabo en ella.
- Dentro de los programas de acceso se puede implementar la característica de que los usuarios solo podrán acceder la terminal a cierta hora del día, teniendo un control total sobre quien esta usando a la maquina a determinada hora.

El control de acceso considerara el proceso de autenticación de usuarios por medio de medidas de software, es decir, por medio del uso de passwords. La autenticación de los usuarios debe considerar varias situaciones: usuarios que escriban mal su passwords, mal funcionamiento del teclado, etc. Para el caso de uso de passwords ciertas medidas pueden ser programadas por dentro del programa controlador de accesos:

- Implementar un pequeño retardo en el proceso de verificación de 5 a 10 segundos. Para un usuario normal este proceso presentara una molestia mínima, sin embargo, para un posible perpetrador de robo de información y acceso no autorizado que use programas de ataque por búsqueda en diccionario, este retardo en cada intento de introducción de password hará que el ataque sea infeasible.
- Determinar el número de intentos de passwords equivocados que puede hacer un usuario. En caso de que sea muy importante para el negocio mantener ladrones fuera del sistema, con tres oportunidades basta. Si se dan las tres entradas equivocadas la cuenta del usuario

debe ser dada de baja y solo el encargado de seguridad puede volverla a habilitar. Esto facilita la identificación de cuentas que están bajo ataque.

- Programar el sistema para que obligue a los usuarios a cambiar de password periódicamente. Para evitar el reuso de passwords algunos sistemas de control de acceso rechazan cualquier password que haya sido usada recientemente.

Una técnica muy recomendable en el uso de passwords es utilizar las llamadas passwords de "uso único" (*one-time password*). Estas cambian cada vez que son usadas. En los passwords de uso único al usuario se le asigna no una frase, sino una función matemática. Aquí el sistema da un argumento para la función y el usuario debe introducir el valor resultante. Un sistema que utilice esta técnica es llamado desafío-respuesta (*challenge-response*) porque el sistema le presenta al usuario un desafío y determina la autenticidad del usuario por su respuesta. Las funciones que se definen para los password de uso único pueden llegar a ser muy complejas, por ejemplo: $f(E(x))=E(D(E(x))+1)$ en donde la computadora envía un valor encriptado $E(x)$ y el usuario debe desencriptar el valor, aplicar la función aritmética $+1$ y encriptar el nuevo resultado para enviarlo de regreso al sistema. Los passwords de uso único son muy seguros ya que si descubren uno, este es inútil.

Estas recomendaciones son hechas pensando en que solo se debe desconfiar del usuario, pero existe el caso en que el sistema ya ha sido comprometido, es muy sencillo crear un programa que muestre o simule el símbolo del sistema y los espacios para el ID del usuario y el password, capture la información escrita y la guarde. En este tipo de ataque el perpetrador escribe el programa, lo coloca en la terminal, espera que alguien escriba su password y se aleja sin que nadie se de cuenta. Las recomendaciones para evitar este tipo de ataque son:

- Asegurarse de reiniciar la ruta del sistema cada vez que se comience a trabajar. En algunos sistemas el presionar la tecla BREAK detiene los procesos que se realizan, o proceder al apagado y encendido de la terminal.
- Para asegurarse que la computadora esta corriendo el sistema que se desea, podemos programar el control de acceso para que antes de introducir password o datos confidenciales, muestre la fecha de la ultima vez que el usuario entró al sistema. Si se desea un mayor nivel de seguridad se puede encriptar el mensaje con la fecha, y el usuario se encargara de desencriptar y verificar la información, si es correcta el usuario encripta la fecha y el password para garantizar que un intruso no haya interceptado el password. Estas encripciones y desencripciones pueden ser hechas con algoritmos del tipo DES.

Si la red local tiene varios servidores de información, se pueden usar los programas de control de acceso para restringir el trafico entre los servidores. Esto se debe especificar en las políticas de manejo de la red local, de modo que el transito de información trivial entre servidores debe ser restringido.

Varias compañías de software se dedican a desarrollar sistemas de control de acceso. El administrador de la red debe tener en consideración algunas situaciones, como por ejemplo:

- Evitar otorgar permisos de escritura a usuarios que solo necesitan permisos para leer archivos importantes
- Implementar un *checksum* encriptado para información delicada.

KERBEROS. Para una red de computadoras existe la opción de elegir un sistema de autenticación de los ya existentes. Kerberos es un sistema que soporta la autenticación para sistemas distribuidos. Para esto hace uso de la encripción por llave pública y llave privada. Kerberos es utilizado para procesos entre sistemas inteligentes tales como, tareas de servidor a cliente, o entre usuarios de las computadoras en la red. Kerberos se basa en tener un servidor central el cual provee de "boletos" autenticados para las aplicaciones que los requieran. El "boleto" es una estructura de datos autenticados definiendo a un usuario y un servicio que el usuario esta permitido a utilizar, contiene valores de tiempo e información de control.

Para empezar a usar Kerberos, primero se tiene que iniciar una sesión con el servidor de Kerberos, la estación de trabajo del usuario envía la identificación del usuario al servidor cuando

este introduce su ID. El servidor de Kerberos se encarga de verificar que el usuario este autorizado y envía dos mensajes: A la estacion de trabajo del usuario le envía una llave de sesión S_G para que la utilice en la comunicación con otro servidor que otorga los "boletos" y un boleto T_G para el servidor de boletos, tipicamente S_G esta encriptado con el password del usuario $E(S_G+T_G,pw)^2$. El otro mensaje que envía Kerberos es al servidor de boletos, envía una copia de S_G y de la identidad del usuario, encriptado con una llave compartida entre Kerberos y el servidor de boletos. Con este intercambio finalizado, si la estación de trabajo del usuario es capaz de desencriptar $E(S_G+T_G,pw)^2$ con el password del usuario, entonces la terminal y el usuario se han autenticado. Con la llave de sesión S_G el usuario puede solicitar boletos para accesar archivos o recursos y el servidor de boletos otorgara los permisos y derechos para el nivel de este usuario.

Kerberos fue diseñado para poder resistir ataques y evitar los accesos no controlados ya que:

- Los passwords son almacenados en el servidor de Kerberos y no en la estación de trabajo y el password del usuario tampoco ha sido enviado por la red.
- Cada petición de acceso es mediada por el servidor de boletos, el cual conoce la identidad de quien hace la petición por el proceso de autenticación que hizo con Kerberos.
- Cada boleto esta limitado a tener validez solo durante determinado tiempo, así, en caso de presentarse un ataque de criptoanálisis por fuerza bruta no hay tiempo suficiente para completar el ataque.
- Kerberos necesita usar un reloj universal ya que cada petición del usuario al servidor queda grabada con la hora en que se hizo. Cuando llega una petición al servidor, este compara el tiempo en que se hizo con el tiempo actual y completa la petición si el tiempo de la petición es razonablemente cercano al actual. Eso previene los ataques por "replay" porque la presentacion del boleto del atacante se retrasa mucho.
- La autenticación mutua permite que el servidor otorgue un canal único al usuario, de manera que el usuario no necesite encriptar las comunicaciones en ese canal. Con menos información que encriptar se ahorra tiempo en las transferencias.

CONTROL DE TRAFICO. En una red de computadoras se tiene información viajando entre terminales y entre servidor y terminal, por tanto se tiene una cantidad considerable de bits en los canales de comunicación. Por ello, el trafico también es blanco de amenazas de seguridad, a esto se le llama **análisis de trafico.** El análisis de trafico no es tan común como otros tipos de amenazas informáticas porque pocos atacantes están dispuestos a analizar todo el trafico de la red y que existen técnicas simples contra este análisis.

Como un interceptor ilegal puede revisar todos los bloques de mensajes que pasan en la red y conocer quien esta en comunicación continua, él se da cuenta cuando el trafico en cierta dirección aumenta con lo que puede adivinar alguna situación especial. El procedimiento simple es que para evitar un notorio aumento de trafico entre ciertas terminales, introducir mensajes "sin uso" en las rutas con poco flujo. El lado negativo de esta técnica es que agrega carga a la red y el servicio a los usuarios puede degradarse.

Otro tipo de ataque es el establecer un canal encubierto en una red generando trafico, incluso trafico "sin uso". En esta técnica se representa un 1 binario con un mensaje hacia un nodo, y un 0 binario ya sea por la ausencia de mensaje o un mensaje enviado hacia otro nodo. Esta incursión en la red no requiere participación activa del intruso. Además de que este trafico puede parecer normal si esta dirigido hacia una terminal razonable, por ejemplo hacia un sistema de archivos. Este tipo de trafico puede permitir una enorme cantidad de información robada. Si en la organización o negocio necesitan un completo confinamiento de la red, el canal encubierto debe ser puesto fuera de circulación. Para ello hay dos técnicas: la introduccion de trafico y el control de ruteo.

La **introducción de tráfico** la acción llevada a cabo por el administrador de la red para introducir ruido entre los pares de terminales comunicándose. Este ruido es generado en forma de mensajes "sin uso" de manera aleatoria sin seguir ningún patrón, frecuencia, fuente o destino. Con este ruido, se espera que se distorsione el flujo de información en el canal encubierto. Las

terminales legales deben ser capaces de reconocer los mensajes falsos para que no interfieran con la comunicación del usuario legitimo. El administrador de red no necesita participar en el trafico de la red mas que para generar mensajes de ruido periódicamente.

Para controlar los canales encubiertos, el administrador de la red puede ejercer un **control activo de ruteo** en la red. Por ejemplo, si el canal encubierto fuera 1 para el mensaje de A a B y 0 para el mensaje de A a C, el administrador puede tratar de redirigir los mensajes, haciendo un nuevo ruteo de los mensajes enviados de A a C para que vayan de A a B y después a C. De este modo, un mensaje A-C (0) sera convertido a un mensaje A-B (1) seguido de un mensaje B-C (sin valor). Si la red maneja algún protocolo para detectar los mensajes perdidos, el administrador puede periódicamente borrar o desviar mensajes. Así, B se dará cuenta hasta mucho después de que un mensaje de A no fue recibido. Si esto pasa, B pedirá una retransmisión del mensaje, la repetición del mensaje no afectara la comunicación normal. El flujo del canal encubierto sera afectado porque otros mensajes ya pueden haberse transmitido, y este mensaje que representa un bit sera transmitido fuera de secuencia. El administrador también puede retrasar los mensajes periódicamente. Con ello es posible que se destruya la sincronización entre la fuente y el intruso sin afectar de manera seria el trafico legitimo. Este tipo de control es muy efectivo si el canal depende del momento de llegada de mensajes.

Estos controles de trafico dependen de un administrador de red activo que pueda efectuar acciones en la red para destruir canales no autorizados y manipular el trafico de la red.

CONTROLES DE HARDWARE

Esta configuración consta de varias computadoras en red. Esto significa que comparten archivos y que por medio de un ***hub*** o de un servidor central están interconectadas. Aquí también se protege el sistema por mas medios que solo programas de software.

BIOS. Al igual que en las configuraciones uno y dos, es necesario proteger las máquinas durante el arranque del sistema. Por ende, se recurre al BIOS. El BIOS contiene los datos de configuración y de información del sistema, al mismo tiempo que varios parámetros ajustables. El orden de los dispositivos de arranque, controlado por el BIOS, es causa de preocupación porque casi todos los sistemas operativos tratan de arrancar primero desde la unidad de discos, después desde la unidad de CD o del disco duro, alguien podría aprovecharlo y reiniciar el sistema desde un disco que contiene código ejecutable para crear puertas traseras en alguna máquina de esta LAN interna. Para la eliminación de esta vulnerabilidad, hay que configurar el BIOS para que arranque desde el disco duro desde la primera vez, y si es posible, eliminar la unidad de disco y el CD-ROM de la secuencia. Posteriormente agregar un password al BIOS. Esto obliga a que se introduzca un password antes de permitir hacer cambios al BIOS y evita que alguien vuelva a cambiar la secuencia de arranque para usar la unidad de disco, al mismo tiempo que nos protege de alguien que quiera evitar el inicio del sistema. Sin embargo, sigue siendo muy sencillo evadir la protección de password en el BIOS. Solo se debe cambiar la posición de un jumper en el motherboard y así la configuración del BIOS volverá a su estado por default deshaciéndose del password. La protección del BIOS depende de los conocimientos que tenga en cuanto a mover el jumper, ya que hay que abrir la computadora y localizar el jumper. Esto afecta a todos los sistemas operativos ya que el BIOS es parte de la arquitectura de la PC.

Si se utiliza el sistema LINUX, existe la opción de utilizar el Linux Loader (LILO), esté se coloca en el registro del master boot del sistema. BIOS le cede la ejecución a LILO. LILO cargara el kernel de LINUX, y este completara el proceso de arranque. LILO permite que se arranque el sistema en un cierto estado de operación ***init.*** Cuando un usuario desea arrancar en el estado 1 (***init state 1***) el requisito de la autenticación es pasado por alto, y se presenta la línea de comandos de la consola con privilegios de raíz. Para poder evitar este problema, se puede agregar un password a la configuración de LILO, la cual se encuentra en el archivo ***/etc/lilo.con***. De esta manera será necesario introducir un password cada que se desee arrancar un sistema operativo, o incluso usar un password distinto para cada sistema operativo disponible. Para prevenir que los usuarios vean la información del archivo, se configuran los permisos para que solo se puedan leer

desde raíz. No hay información acerca de que algún otro sistema operativo otorgue la posibilidad de asegurar la información del BIOS. Toda esta reconfiguración y protección del BIOS debe hacerse en cada computadora de la red. En algunas ocasiones puede ser un proceso largo y tardado pero hay que hacerlo si realmente se necesita un sistema protegido de cualquier vulnerabilidad. Los responsables de implementar estos cambios serian el administrador de red o el encargado de la seguridad informática.

SMARTCARD. En esta configuración de sistema se pueden usar las smartcards (tarjetas inteligentes), las cuales generan cada determinado tiempo un password que permite el acceso hacia las áreas de la información critica que contiene la PC o alguna base de datos de esta red. Si no se tiene, el acceso es prácticamente imposible ya que el password que genera esta formado por letras y números de distinta longitud y obliga a ataques por fuerza bruta. Muchos negocios utilizan técnicas de autenticación biométrica en conjunto con smartcards; las técnicas biométricas miden alguna característica física única del usuario, tal como el patrón de la voz, de cara, el orden de los vasos sanguíneos de la cornea y las huellas digitales. Tradicionalmente, las representaciones digitales de las características biométricas ocupan un espacio entre 100 y 600 bytes y por ello se pueden acomodar en una smartcard. Los pasos característicos de una autenticación de usuario por medio de smartcard y medidas biométricas son los siguientes:

1. Insertar la smartcard en el lector, esta contiene las llaves criptográficas y los datos correspondientes a la huella digital del usuario.
2. Se introduce el número de identificación privada (PIN), así, se libera la representación electrónica de la huella digital.
3. Ahora se coloca el dedo en el escáner, esta huella es comparada con la guardada en la smartcard.
4. Si la comparación es positiva, los datos de la huella en la smartcard son convertidos a un valor numérico y se combinan con el PIN de la smartcard para formar una llave de encripción simétrica la cual desencripta la llave privada.
5. Un número aleatorio es generado por la computadora donde se conecta la smartcard, este número es transferido a la smartcard.
6. La llave privada en la smartcard es usada para encriptar el número aleatorio y mandarlo de vuelta a la computadora.
7. La computadora verifica que una llave pública certificada obtenida de algún directorio en red desencripte el número aleatorio y verifica que este sea el mismo que se envió originalmente a la smartcard.

Este proceso se encarga de autentificar de manera irrefutable al usuario de la smartcard. Cada usuario con acceso a estas computadoras debe de contar con su propia smartcard. Aquí también seria el administrador de la red quien estuviera a cargo de la actualización y entrega de smartcards.

PUERTOS INFRARROJOS. Para la tercera configuración de sistemas informáticos se pueden aplicar los mismos métodos para proteger los puertos infrarrojos. En esta configuración de computadoras conectadas en red las vulnerabilidades son iguales que para computadoras individuales: riesgo de sobreflujo del buffer y reinicio del sistema, copiado de archivos sin autorización, intentos de acceso. Para protegerlas, las medidas son las siguientes:

- Descargar los parches y actualizaciones que cubran esta vulnerabilidad y que ya están disponibles
- Hay que deshabilitar los dispositivos infrarrojos si no están en uso, no basta con deshabilitar la comunicación, sino que hay que deshabilitar todo el dispositivo utilizando el programa Administrador de Dispositivos
- Asegurarse que los puertos infrarrojos tienen bloqueada la línea de vista

También se puede colocar cinta opaca sobre el puerto aunque esto solo servirá si el oponente no tiene acceso a la máquina. Estas precauciones deben tomarse en cada una de las máquinas de la red que contengan puertos infrarrojos.

POLÍTICAS

En la configuración tres tenemos una red de computadoras. Estas no tienen conexión a Internet, de igual manera deben de definirse ciertas políticas de seguridad, ya que los riesgos aumentan al tener varias computadoras conectadas en red, debemos de recordar que si un pirata tiene acceso a alguna computadora de esta red puede poner en riesgo la información manejada por toda la red. Antes de enunciar políticas dentro del negocio o compañía se deben establecer los lineamientos de uso, hacer un análisis de riesgos en el sistema y definir una estructura para el equipo de seguridad. Los lineamientos de políticas deben encargarse de contestar las preguntas: ¿A QUIEN se le permite acceso? ¿A QUE recursos? y ¿COMO se regula el acceso?. Las políticas también deben especificar: las metas en seguridad de la organización, quien tiene la responsabilidad de la seguridad, y el compromiso de la organización con la seguridad. En esta configuración se tienen varias computadoras conectadas en red, se pueden imponer las siguientes políticas, aunque estas dependen de las necesidades de seguridad del negocio ya que las políticas se pueden hacer más restrictivas o más libres.

- Cada cierto tiempo los usuarios deben cambiar los passwords de inicio de sesión en la red y de inicio del sistema.
- Los usuarios no deben utilizar el nombre propio o apellido como clave de acceso, ni el nombre de la pareja, hijo o mascota.
- Antes de tener acceso a cada terminal el usuario debe autenticarse por medio de lectura de su huella digital del pulgar derecho y la introducción de su password privado.
- El administrador de la red o el equipo de seguridad debe efectuar auditorias frecuentemente con los programas correspondientes para estar al día en cuanto a vulnerabilidades en redes.
- Los usuarios de las redes no deben escribir los passwords en ninguna lista o papel.
- Los usuarios deben ser instruidos para utilizar distintos passwords para cada aplicación, inicio del sistema, o inicio de sesión en red.
- Para no arriesgar la información confidencial, esta debe ser almacenada en forma encriptada.
- Los monitores y las impresoras deberán colocarse en lugares donde la visibilidad de su información le sea imposible a otras personas que transiten por esos lugares.
- Todas las computadoras deben de arrancar directamente del disco duro y ninguna de ellas debe contar con unidad de discos.
- Los usuarios de la red no deben revelar a gente no autorizada las claves de acceso a la red.
- Los usuarios deben desactivar los puertos infrarrojos de la terminal cuando no estén en uso.
- La firma de cláusulas explicitas dentro de los contratos de los trabajadores en donde acepten el no revelar información a competidores. Y así poder emprender acción legal en caso de que violen este convenio.

Las políticas de seguridad son reglas que nos dictan como conservar la seguridad y las acciones a tomar en caso de una ruptura a la seguridad e incursión dentro de la maquina que queremos proteger.

CONTROLES FÍSICOS

AUTENTICACIÓN BIOMÉTRICA. La configuración tres consiste en una red de computadoras, aquí también podemos utilizar las técnicas biométricas para evitar el acceso a computadoras o a los edificios y oficinas donde se encuentran las computadoras conectadas a la red. Se pueden emplear los siguientes métodos de protección:

- Revisión de retina
- Las técnicas de reconocimiento de voz y de firma de usuario, aunque estas no son biométricas

- Técnicas de autenticación de rostro, mano o huellas digitales

Antes de aplicar estas técnicas hay que investigar si todas las computadoras se encuentran en la misma oficina o en oficinas separadas, y si será necesario instalar el equipo para el control de acceso a cada una de estas máquinas u oficinas y al cuarto donde se encuentre el administrador de la red. El uso y aplicación de estas técnicas depende de evaluar previamente varios factores: nivel de seguridad que se necesite, costo y tiempo de implementación, aceptación de los usuarios y confiabilidad.

- Nivel de seguridad. El reconocimiento de voz y de firma son técnicas aceptables cuando se habla de usos no relacionados con autorización de acceso a la PC, sin embargo son útiles para la autenticación de usuarios de la red o de la PC. Las técnicas biométricas que identifican características físicas son más confiables y otorgan un nivel mayor de seguridad.
- Costo y tiempo de implementación. Cuando se desea implementar un sistema de autenticación biométrica de usuario, se debe de hacer en conjunto con el proveedor de computadoras y tomar en cuenta que hay que buscar e instalar el software y hardware compatible con la PC para autenticación (cámaras, lectores, *scanners*), el software y hardware necesarios para mantener la base de datos de usuarios, el tiempo que se lleva integrar el hardware de autenticación en el ambiente de trabajo, el entrenamiento del staff para manejar el nuevo sistema, el entrenamiento de los usuarios con el nuevo protocolo de autenticación y la actualización continua de las bases de datos.
- Aceptación de usuarios. Los usuarios generalmente aceptan las técnicas que son menos intrusivas o gorrosas, tales como identificación de huellas, rostro o mano. Aquí es responsabilidad de la organización el entrenar a los empleados para que se familiaricen con los nuevos requerimientos antes de que el sistema sea implementado.
- Confiabilidad. La revisión de retina e identificación de iris son altamente eficientes para identificar individuos, sin embrago, son muy costosas y la mayor parte de los negocios no necesitan este nivel de confiabilidad. Técnicas de autenticación de huellas, mano, y rostro ofrecen buena confiabilidad y requieren una menor inversión en equipo de revisión. Los cambios físicos tales como cortadas, cicatrices y el envejecimiento pueden afectar la identificación, sin embargo las bases de datos se pueden actualizar.

Existen dos términos que describen la funcionalidad de las técnicas biométricas: la razón de falsa aceptación (*False Aceptance Rate*, FAR) el cual describe la probabilidad de que un intruso sea aceptado con una medida que no le pertenece de un usuario enrolado. La razón de rechazo falso (*False Rejection Rate*, FRR) es la probabilidad con que un usuario enrolado sea rechazado. Se considera que un buen equipo biométrico tiene un bajo FRR y FAR. Casi siempre hay un intercambio entre seguridad y conveniencia, en los sistemas biométricos mientras más seguro el sistema (mas bajo FAR) es más inconveniente para el usuario, ya que ocurren más rechazos falsos. Similarmente, mientras más conveniente sea el sistema, menos seguridad tiene. Los sistemas biométricos le permiten al usuario elegir entre un amplio rango de niveles de FAR/FRR.

Tomando en cuenta que puede haber ocasiones extremas en donde se utilice un dedo cortado de la mano o dedos falsos. Algunos vendedores miden el calor del dedo en el escáner, otros miden su conductividad para evitar casos donde se modifiquen las huellas con silicón. La solución más adecuada es por medio de la medición **espectroscópica** de la cantidad de hemoglobina oxigenada en la sangre, ya que es imposible de pasar con dedos artificiales y los resultados de esta prueba son muy distintos para dedos vivos y dedos cortados.

En esta configuración se puede presentar muchos gastos ya que quizá sea necesario proteger cada una de las computadoras y todo depende del tamaño de la red que puede ser de unas cuantas computadoras hasta varias decenas.

HERRAMIENTAS Y MEDIDAS FÍSICAS. Consideramos también en los controles físicos las estrategias y herramientas que ayudan a impedir los incidentes de robo o perdida de equipo de computo. En esta configuración tenemos una red de computadoras, así que las medidas de seguridad física que se recomiendan son:

- Designar un oficial de seguridad departamental, quien reportara rupturas en la seguridad y actos ilegales. Además será el responsable de implementar, coordinar, mantener y monitorear un programa de seguridad departamental.
- Debe restringirse el acceso a los gabinetes y closet donde se encuentran el cableado de las conexiones, los servidores de archivos y ruteadores.
- Establecer puntos de recepción en el edificio entre áreas funcionales o zonas seguras.
- Definir claramente los limites del acceso público en el edificio, por medio de señalamientos.
- Si es posible colocar todas las computadoras en una sola oficina para que solo se proteja una vía de acceso a ellas y así evitar grandes gastos en la aseguración de múltiples oficinas.
- Instalar puertas y ventanas que den entrada al edificio u oficina donde esta cada computadora de la red, las cuales deben contar con alarmas contra apertura o ruptura.
- Los cables de aseguramiento de computadoras son muy populares hoy en día y pueden ser otra opción en lugar del gabinete, así como placas de acero para aseguramiento de cada computadora de la red que la mantiene fija en su lugar.
- Vigilar frecuentemente que no haya algún cable superpuesto al cable que permite la conexión a la red de cada computadora.
- Para evitar el acceso a las unidades de disco de las computadoras se emplean candados con llave, esto puede llevarse a cabo por los guardias o los mismos usuarios de las terminales al finalizar su jornada de trabajo.

Todas estas medidas son para prevenir el robo y destrucción, aunque se puede idear medidas más estrictas dependiendo de los requerimientos de la empresa.

NIVEL DE SEGURIDAD

En la configuración tres se cuenta con una red de computadoras sin conexión a Internet. Antes de aplicar las recomendaciones, el nivel de seguridad es **1** si el sistema cumple con protección antivirus y protecciones contra robo físico.

Su operatividad es alta ya que los métodos de seguridad son mínimos:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{1} = 1$$

Con las recomendaciones hechas en los apartados de **encripción, Controles de Software, Controles de Hardware, Políticas** y **Controles Físicos** se cubren las características descritas para la obtención del nivel **4** de seguridad. Este sistema no logra obtener el nivel 5 debido a que no cuenta con conexión a Internet y por tanto, no se aplica la protección contra accesos externos no autorizados.

Su nivel de operatividad esta determinado por la formula:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{4} = 0.25$$

El nivel de operatividad es bajo, obviamente esto depende de las necesidades en seguridad de la empresa o negocio. Si se desea un mayor nivel de operatividad, hay que buscar que servicios de seguridad de los propuestos no son necesarios para la operación del sistema de configuración tres y descartarlos.

Tabla 4.4 - Niveles de Seguridad y Operatividad

Nivel de seguridad por default	**1**
Nivel de Operatividad por default	**1**
Nivel de Seguridad con recomendaciones	**4**
Nivel de Operatividad con recomendaciones	**0.25**

Con las definiciones de seguridad de los niveles en el Orange Book de la página 22 se puede notar que el nivel para el sistema descrito en la configuración tres después de aplicar las recomendaciones y con una correcta implementación de las políticas, control de accesos y autenticación, sería aproximadamente el nivel **B3**. Esto es porque en las recomendaciones de seguridad se tocan los puntos de seguridad autenticada, empleo de un administrador de sistema, diferencias para recursos de usuario y recursos de administrador, capacidad de auditorias, recomendaciones de encripción para comunicar la información entre terminales de la red, restricciones de acuerdo a usuarios y políticas, y protección por hardware también aplicada. El cubrir las características del nivel B2 depende de la etiquetación de objetos y eso puede variar en diferentes sistemas por la información y recursos que se manejen, así que bien puede ser cubierto y bien puede no serlo, depende del administrador. Así, el sistema muestra un nivel de seguridad aproximado muy elevado, solo por abajo del nivel A.

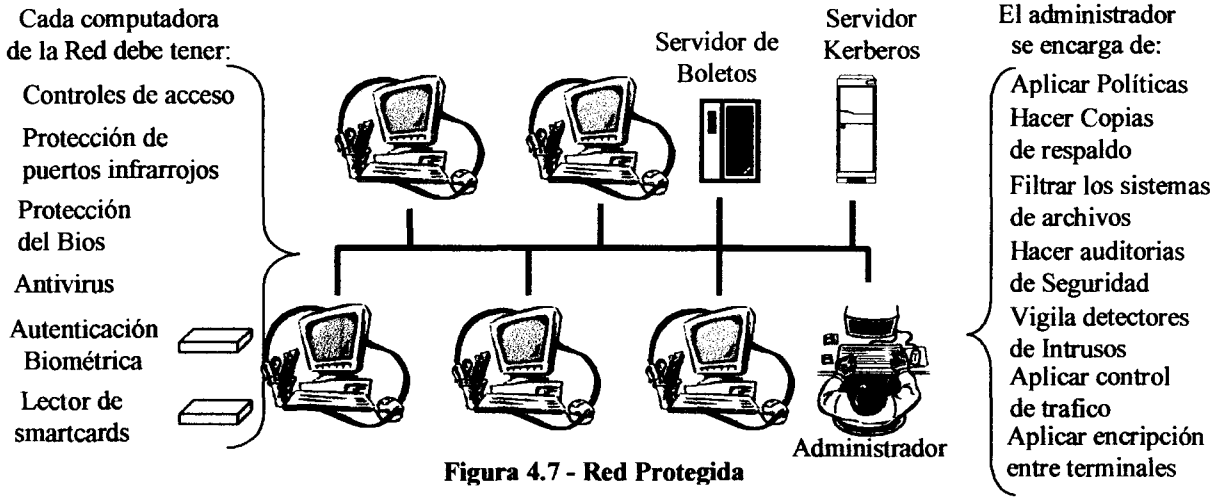


Figura 4.7 - Red Protegida

CONFIGURACIÓN 4 - Red de computadoras con conexión a Internet

Otro ejemplo de un sistema que puede ser susceptible a los ataques informáticos es una red de computadoras conectadas en red y con una puerta de entrada/salida a Internet. Si este tipo de sistema se presenta, los riesgos son mayores ya que la conexión a Internet de las terminales indica una puerta de entrada a amenazas externas. Las características por default de seguridad de una red de computadoras con conexión a Internet consisten en: no tener un administrador de red o responsable de seguridad, sistemas operativos sin parches de seguridad instalados, ningún tipo de autenticación de usuario o codificación para proteger archivos importantes o el acceso a la red, servicios de red disponibles para personal no autorizado, ningún software de auditorias, falta de software o dispositivos que eviten las incursiones al sistema desde Internet, tampoco detectores de intrusos, además de tener casi todas las características de seguridad para operación en red de los sistemas operativos al mínimo por default. Muchos de los equipos de computo vienen de fabrica con programas antivirus instalados (no necesariamente actualizados) y candados o elementos de seguridad física para cada computadora y servidor utilizado, como se trata de una red es posible

que todas las computadoras estén en un solo lugar y se asegure el cuarto con llave. La poca seguridad existente es física y los peligros de robos de información siguen estando presentes.

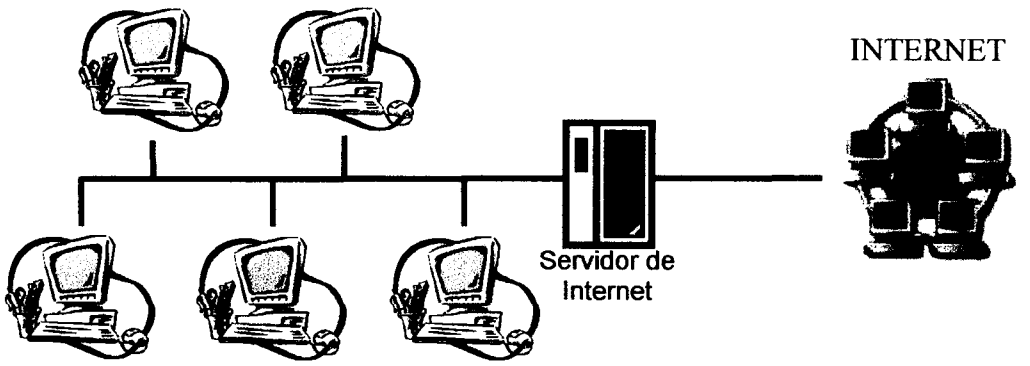


Figura 4.8 - Una red con conexión a Internet

Para evitar estos problemas y filtraciones en la seguridad se hacen algunas sugerencias que son muy parecidas a las expuestas en la configuración tres, y se incluyen los aspectos necesarios para contrarrestar las vulnerabilidades de la conexión a Internet.

ENCRIPCIÓN

Las recomendaciones de encripción son similares a las hechas para la protección de la información en la red de la configuración tres. Debido a los riesgos existentes, es normal que se opte por asegurar la información en las redes encriptandola y en combinación con otros controles. En el ambiente de red, donde el trafico entre terminales o hacia fuera de la red es muy grande, la encripción puede ser de mucha ayuda, en caso de que los archivos transmitidos sean interceptados permanecerán seguros y se necesitaran ataques de criptoanálisis para descifrarlos. El problema con la encripción es el uso de llaves, ya que estas deben ser enviadas a la fuente y receptor de los mensajes.

En la encripción de enlaces (*link encryption*), la información es encriptada justo antes de que el sistema la coloque en el enlace de comunicaciones. En este caso la encripción se lleva a cabo en las capas 1 y 2 del modelo OSI. La desencripción ocurre justo cuando la información entra en la computadora receptora. En este método la encripción protege el mensaje en transito entre dos computadoras, sin embargo, el mensaje esta en texto simple dentro del anfitrión y en las capas superiores a la capa 1 dentro de la terminal fuente y la receptora. Incluso si el mensaje tiene que pasar por algún anfitrión, él también podrá verlo de manera simple y no encriptado ya que las tablas de ruteo y direccionamiento no se leen en la capa física, sino en las de enlace y de red. Esto puede crear un problema de seguridad si el anfitrión no es confiable o su seguridad ha sido comprometida. La encripción de enlace es invisible al usuario y es llevada a cabo por un protocolo de capa de red de bajo nivel. En un mensaje encriptado de esta manera los encabezados (*header*) y la información de control son agregados por el lado del origen y removidos en el lado del receptor. Como la encripción se lleva acabo en la capa mas baja, no solo el mensaje es encriptado, sino los encabezados de transporte, red y sesión. El uso de este método se recomienda si los riesgos de seguridad son mayores en las líneas de comunicación.

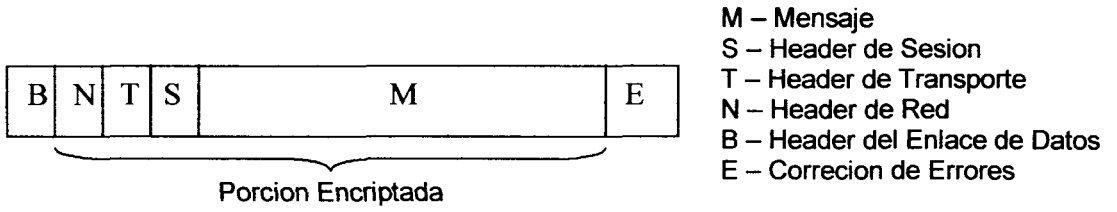


Figura 4.9 - Mensaje con encripción de enlace

Otra forma de proporcionar seguridad a una red por medio de la encripción es con el método de terminal a terminal (*End-to-End Encryption*). Este provee encripción por un dispositivo de hardware entre el usuario y el host. Una alternativa para esto, es la encripción realizada por software en la propia computadora. De cualquier manera, la encripción se realiza en las capas 7 o 6 del modelo OSI y por ello solo encripta el mensaje y no sus encabezados. La encripción asegura que el mensaje este encriptado para cualquier capa, así, si el mensaje es interceptado en su transcurso hacia otro punto seguirá estando encriptado.

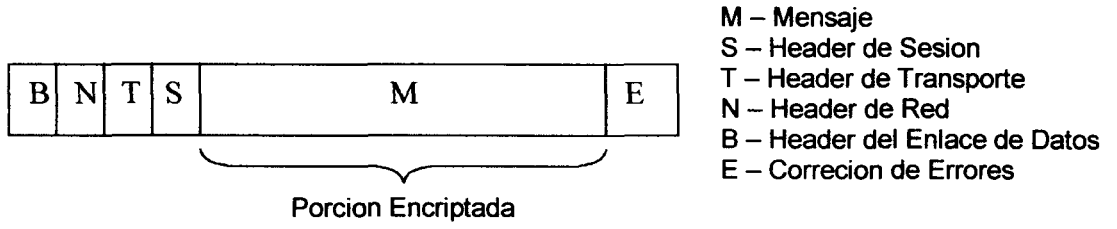


Figura 4.10 Mensaje con encripción de terminal a terminal

La encripción de enlace es más rápida, más fácil para el usuario, y utiliza pocas llaves, ya que solo requiere una por cada par de terminales. La encripción de terminal a terminal es más flexible, puede ser usada de manera selectiva y como es a nivel usuario se puede efectuar dentro de la aplicación. Esta características es muy útil para una red con conexión a Internet, si un intruso lograse entrar a la red y revisar el trafico con la intención de atrapar la información importante, la encripción de ella hará necesario gastar más recursos para entenderla y al mismo tiempo, la encripción de los archivos puede hacer que sean difíciles de identificar para su intercepción.

Si los recursos lo permiten y existe el caso en que no se confíe en las otras terminales anfitriones dentro de la red se pueden utilizar los dos tipos de encripción. Si no toma mucho tiempo la encripción de datos, entonces las molestias y rendimiento negativo sera poco.

Otro de los casos donde la encripción es de utilidad es para codificar la información critica almacenada en discos, CD, archivos en disco duro, etc. Para este almacenamiento se puede optar por encripción simétrica, si solo una persona esta a cargo de su almacenamiento, encripción y desencripción. Sin embargo, si los archivos de respaldo se envían de un lugar de la red a otro, la encripción asimétrica sera la mas indicada ya que se efectuaría con la llave pública del receptor y su desencripción haría uso de la llave privada del receptor también.

CONTROLES DE SOFTWARE

En la configuración cuatro de sistemas de información, se debe proteger la red de amenazas externas e internas. Desde el exterior pueden buscar acceso por la conexión a Internet de la red virus, *worms*, *trojans*, intrusos, accesos piratas, tráfico falso, etc. De igual manera, se tienen aun las amenazas desde el interior de la red mencionadas para la configuración tres, donde encontramos usuarios que tratan de ganar privilegios extras, monitoreo de trafico en la red,

falsificación de trafico, virus, etc. Enseguida se presentan las recomendaciones en distintas áreas de software para la protección de la red con conexión a Internet.

PROGRAMAS AUDITORES. Una de las opciones para la protección de una red de computadoras es la utilización de programas para la seguridad de la información, tales como software para la administración de eventos de seguridad, para el escaneo de vulnerabilidades en el sistema o proveedor de servicios de seguridad. El software para la administración de la seguridad de una manera centralizada se esta volviendo la forma más popular entre los administradores de red para estandarizar y analizar la información concerniente a eventos de seguridad en una sola consola central. Los programas auditores se encargan de revisar la condición y administración de los puntos de seguridad de la red. En la configuración 4 de sistemas, los programas auditores nos darán la siguiente información del sistema:

- Las vulnerabilidades que tiene la red al estar en línea y actualizaciones recomendables para los programas utilizados. Cualquier programa que tenga capacidades de conectarse en línea o de recibir información por medios externo puede representar un problema de seguridad al entrar en línea. Muchos atacantes solo esperan la oportunidad de que cierto programa con vulnerabilidades conocidas se conecte a Internet.
- El flujo de datos a través de los dispositivos y agentes de seguridad instalados en puntos estratégicos de la red (en la entrada de Internet, en la línea principal de la red, a la entrada de la terminal que maneja información critica) y los reportes de los controles de seguridad.
- La información contenida en los reportes de los programas auditores debe incluir aquella sobre cualquier usuario o entidad en la red que trate de obtener un nivel de seguridad mas elevado, información sobre accesos y salidas del sistema, accesos de superusuario, y cualquier otro cambio de acceso o estatus.
- Una medición de la eficiencia en las operaciones, por ejemplo, virus detectados en la red vs los eliminados, virus detectados en las terminales vs los eliminados.
- Una evaluación del apego a las políticas de seguridad o estándares, por ejemplo, los estándares en antivirus especifican que todos los archivos ***.DAT***, donde se mantiene la información de nuevos virus, deben ser descargados de Internet cada cierto tiempo.
- Los programas auditores permiten establecer las bases para un plan comprensivo de respuesta a incidentes de seguridad.

El tipo de información recopilada es distinta para cada sitio y configuración, estando limitada la recopilación solo por el espacio disponible para su almacenamiento. La información generada por los programas auditores puede almacenarse de varias formas: en archivos de lectura y escritura dentro de la terminal de monitoreo central, en un dispositivo donde se escribe una vez y se puede leer varias (CD-ROM), o en un dispositivo de solo escritura (impresora de línea). Cada una de estos métodos tiene sus ventajas y desventajas. Si se elige grabar los registros en un archivo de lectura-escritura dentro de la terminal donde se concentra la información de los reportes, se tendrá acceso instantáneo a los registros para su análisis en el momento de un ataque, por otro lado, es poco confiable ya que, si alguien logra acceder a este sistema por algún método y su intención es robar información, modificarla, o falsificarla, puede fácilmente borrar cualquier dato de la intrusión al manipular los archivos del registro. La segunda opción es guardar la información en un medio donde se escriba una vez, como un CD; esto es un poco más complicado de configurar, la información no estara disponible instantáneamente y el costo es más elevado, aunque es un método mas seguro ya que, un intruso no podrá modificar los archivos en un CD para cubrir su intrusión. La tercera opción para el almacenamiento de la información de auditoria es con un dispositivo de solo escritura, tal como una impresora de línea; este método es de mucha utilidad si se requieren registros permanentes e inmediatos para el caso donde se quiere saber el punto exacto de una falla o ataque al sistema; si se quiere usar una impresora laser o algún otro dispositivo que ponga la información en espera se puede perder la información en el momento critico; las desventajas de este método son el mantener alimentada con papel la impresora y donde guardar todo el papel utilizado para un análisis posterior. La información de los programas auditores puede ser clave para la investigación, detención y proceso legal de los

responsables de robo informático. Algunos ejemplos de programas que sirven para hacer auditorias de seguridad son: ***LT Auditor+ Version 8.0, Nessus, Nmap***.

PROGRAMAS ANTIVIRUS. Para una red de computadoras existe el riesgo de que si una de las maquinas es infectada por un virus toda la red puede ser victima, los virus informáticos están presentes y pueden llegar de manera accidental o intencional a la red, ya sea por medio de un archivo enviado de una terminal a otra, al compartir una aplicación infectada, por medio de un disco contaminado, al abrir un correo electrónico, navegar páginas no seguras por Internet o recibir el virus disfrazado. El software antivirus debe ser instalado en cada una de las máquinas de la red si estas cuentan con disco duro, si las terminales no cuentan con disco duro es fácil deshacerse de los virus. Enseguida se presentan recomendaciones de seguridad para tratar con la amenaza de los virus:

- Utilizar solamente software adquirido de vendedores confiables y bien establecidos.
- En caso de que se deba usar software proveniente de fuentes de calidad y honradez desconocidas, se recomienda probar este nuevo software en una computadora separada de la red, que no contenga disco duro ni disco de arranque. Se debe observar el comportamiento del software y buscar cualquier falla e indicios de actividad inexplicable en pantalla. Posteriormente hay que revisar la computadora de prueba con un programa detector de virus, diversos programas antivirus permiten crear un disco de detección.
- Crear un disco de arranque y mantenerlo seguro. Es necesario mantener este disco protegido contra escritura durante el reinicio del sistema.
- Crear y conservar copias de respaldo de los archivos ejecutables del sistema. Así, en caso de una infección, los archivos afectados pueden ser removidos y reinstalados de las copias limpias.
- Utilizar detectores (scanners) de virus regularmente. Muchos de los detectores disponibles hoy en día permiten la detección y la eliminación de los virus. Se recomienda tener mas de un detector porque uno puede encontrar virus que otros ignoran.
- Es una practica popular el enviar virus disfrazados de correo electrónico, por lo que no se deben abrir correos de personas desconocidas.
- Ciertas páginas de Internet creadas por piratas o modificadas por ellos, pueden causar la infección de virus, de modo que lo recomendable es no abrir páginas que presenten este tipo de riesgos. Si existe la necesidad de hacerlo hay que activar la protección en tiempo real que ofrecen los programas antivirus y aumentar el nivel de seguridad del navegador para que se evite la grabación de archivos en el disco duro sin el consentimiento del usuario.

Las amenazas por virus informáticos no infectan un solo tipo de computadora o sistema operativo. Las PC son las más populares y por ello las que más sufren por virus, pero eso no significa que los propietarios de estaciones de trabajo de UNIX, LINUX, Macintosh estén exentos a estos riesgos. Los virus representan amenazas para cualquier programa almacenado sin protección contra escritura. Si las terminales de la red utilizan disco duro y sistema operativo se pueden aplicar las opciones de proteger los archivos contra escritura designándolos como "oculto" o "solo escritura", sin embargo, este tipo de protección puede ser superada por los programadores de virus fácilmente. Es incorrecto pensar que los archivos de información, listas, hojas de trabajo, y demás están a salvo de ser infectados. Los virus no solo se limitan a infectar los archivos de programa sino también afectan a los archivos de datos, esto lo logran al agregar a archivos de texto o de hojas de calculo ciertos comandos de inicio y así esparcen la infección o causan estragos. Si una terminal de la red ha sido infectada hay ocasiones en que un simple apagado general y encendido de la maquina libra del problema ya que los virus residen en memoria y al ser una memoria dinámica se pierde su contenido cuando se corta la energía, aunque se debe tener en cuenta que este método no funcionara si el virus esta guardado en disco o si se encuentra ya en el sector de arranque. Se deben tener muchos cuidados para mantener un sistema funcional y al mismo tiempo protegido de los virus.

FIREWALLS. La configuración cuatro de sistemas puede apoyarse para su protección en el uso de los *firewalls*. Un *firewall* nos permite controlar el acceso externo a elementos que se encuentran detrás del lugar donde esta ubicado el *firewall*, esto significa que podemos evitar ataques externos e intentos de envío de archivos no deseados. El *firewall* es un proceso que filtra el trafico entre su posición y la red exterior, esto lo hace al aplicar ciertas políticas, como puede ser evitar el acceso del exterior y alternativamente permitir el acceso al exterior de ciertas aplicaciones. Parte del reto de instalar un *firewall* es definir de manera apropiada para las actividades de nuestro sistema las políticas en que se basara el filtrado y un cuidadoso posicionamiento del *firewall* dentro de la red, así podemos asegurar que todos los accesos a la red deben pasar por el *firewall*, a esta característica se le llama "siempre-invocado". Existen tres dispositivos que responden al nombre de *firewall*: un *screening router*, el *proxy gateway*, y el *guard*.

El *screening router* es el tipo más útil de *firewall* para algunas situaciones. El ruteador se posiciona en la entrada de la red y él se encarga de dirigir los paquetes de información hacia su destino después de consultar las tablas de ruteo almacenadas. Posteriormente el ruteador envía los paquetes a uno de varios puertos físicos que llevaran el paquete a su destino. Un paquete es una subunidad de comunicación de unos cuentos cientos de bytes, un ruteador puede manejar miles de paquetes por segundo, por estas razones las reglas y políticas establecidas para el monitoreo de este firewall tienen que ser de rápida aplicación de modo que el trafico no sea haga lento. Los *screening routers* tienen la capacidad de verificar que los paquetes provengan de otras terminales en el interior de la red y que la dirección indicada en el campo de fuente del paquete no haya sido falsificada. Esta es una practica popular ya que permitirá enviar trafico exterior hacia dentro de la red, para evitarlo se configura el ruteador para que no permita la entrada a los paquetes externos que presumen de venir de una dirección interna. Los ruteadores también pueden ser configurados para que las terminales internas solo puedan recibir información externa para la transferencia de correo electrónico, esto lo hacen porque los protocolos para transferencia tienen puertos definidos, y en los campos de fuente y destino de los paquetes se indica al final de la dirección de red el número de puerto.

El *proxy gateway* es un *firewall* que simula los efectos correctos de una aplicación de manera que la aplicación verdadera solo recibirá peticiones para actuar de manera correcta. Un *proxy gateway* funciona de manera que para la red interior parece el destino exterior y para la red exterior responde tal y como si fuera la red interior. Esta capacidad le permite al *firewall* monitorear y revisar los comandos del protocolo de un mensaje o de paquetes que quieren viajar a la red interna. La distinción principal entre el *proxy* y el *screening router* es que el primero interpreta el flujo de protocolo hacia una aplicación para que controle las acciones a través del *firewall* basándose en las partes visibles dentro del protocolo y no solo basándose en los datos del encabezado externo.

El *firewall* tipo *guard* se comporta de forma similar al *proxy*. Recibe unidades de datos de protocolo, los interpreta, y pasa a través de las mismas o distintas unidades de protocolo que logran un mismo resultado o modificado. El *firewall guard* se encarga de decidir que servicios ejecutar en nombre del usuario basándose en su actividad anterior con el usuario externo. El grado de control del *firewall* depende de lo que sea computable. El código con que se configura este tipo de *firewalls* es más complejo que los anteriores y por lo mismo más errática.

Se debe recordar que un *firewall* no protege a los datos que salen del ambiente guardado. Además, para los piratas o crackers que navegan en la red, el *firewall* es el elemento visible hacia el exterior y por tanto puede atraer atacantes, por eso se recomienda no solo confiar en un solo *firewall*, si realmente se quiere tener medidas de seguridad fuertes se pueden instalar diferentes capas de protección llamadas ***defense in depth***. Los *firewalls* pueden resistir ataques pero no son impasables, por esto los diseñadores los mantienen pequeños para no dar herramientas extras a un atacante, es muy importante configurar correctamente los *firewalls*, esa configuración debe ser actualizada si cambia el ambiente interno del *firewall*, los reportes de actividades del *firewall* deben ser revisados periódicamente. Los *firewalls* tienen poco control sobre el contenido que se admite dentro del ambiente así que este debe ser controlado por otras herramientas de seguridad. Los *firewalls* deben estar bien aislados, y para ello tienen que ser instalados en una computadora

aparte y con conexiones solo al interior y exterior de las redes, esto permite que el *firewall* presente la característica de "a prueba de alteraciones indebidas".

PROTOCOLOS Y SISTEMAS DE ARCHIVOS. En la configuración cuatro se tiene una conexión a Internet por lo que se envía información hacia fuera de la red y se recibe información desde el exterior. Por ello, hay varios protocolos y sistemas de archivos que pueden usarse para un mejor uso de las capacidades de una red. Se presentan recomendaciones de seguridad para los protocolos de transferencia en redes y compartición de archivos, y para los protocolos que usan la conexión a Internet.

- **FTP**. El protocolo de transferencia de archivos permite a un usuario transferir archivos de texto o binarios entre dos computadoras en red por medio de los puertos 20 y 21. El protocolo FTP utiliza una estructura cliente-servidor con un programa cliente abriendo una sesión en un servidor. Existen muchos servidores anónimos en Internet que le permiten a uno descargar información sin necesidad de autenticarse. Si este mismo servidor permite la grabación de archivos entonces puede ser utilizado para distribuir software ilegal o dañino. Un servidor de este tipo podría ser fuente de virus, troyanos o gusanos informáticos es por ello que solo se debe permitir el uso del protocolo a ciertos sistemas a través del *firewall* de la red. Debe tenerse cuidado con la información descargada de un servidor, y se recomienda revisarla con programas antivirus siempre y en la medida de lo posible probar antes el software descargado en una computadora fuera de la red.
- **TELNET**. Esta es una aplicación que permite a los usuarios entrar en una computadora remota. Telnet transmite toda la información entre computadoras sin encriptar (incluso el nombre de usuario y password). Si un atacante se coloca en la ruta de estos mensajes, podría monitorear toda la información y capturar datos sensibles. Algunos piratas podrían robar la sesión existente de Telnet, si esto sucede, el pirata tendría a su disposición todos los recursos disponibles para un usuario autorizado. Para evitarlo, se recomienda utilizar un esquema de encripción con Telnet y de filtrado a través del *firewall* de modo que solo se le permita el acceso a ciertos sistemas autorizados.
- **LPD**. El daemon para impresora de línea (*Line Printer Daemon*) permite que computadoras en red tengan acceso a los servicios de impresión en otra computadora. Si se permite a los paquetes de LPD (paquetes destinados al puerto 515) ser impresos en un servidor interno de impresión desde fuera de la red local (Internet), se presenta una vía para que un pirata niegue los servicios de impresión a los usuarios internos de la red y monopolice la impresora. Esto se puede evitar aplicando limitaciones, tal como la cantidad de tiempo que la impresora puede ser usada, la hora del día que se usa, etc. Esto también se puede evitar al prevenir cualquier acceso externo a la impresora.
- **NFS**. El sistema de archivos en red (*Network File Systems*) permite la compartición de disco duro entre computadoras. Esta característica es de utilidad para los casos en que las terminales de la red no tienen disco duro y dependen de un servidor de discos para sus funciones de almacenamiento. En el servidor de NFS debe especificarse a que terminales se les enviara la información. NFS no debe exportar o permitir conexión de cualquier terminal fuera de la red y cualquier intento de conexión externa al sistema debe ser detenido por el firewall.
- **NIS**. Los servicios de información en red (*Network Information Services*) funcionan de manera parecida a una aplicación cliente-servidor donde el servidor provee de información de usuarios y computadoras en la red. El sistema NIS provee de un sistema de archivos con password central para redes de computadoras. Existe la posibilidad de que un pirata externo le informe a un cliente NIS que debe utilizar otro servidor NIS para que autentifique su entrada. Si esto tiene éxito el pirata habrá ganado acceso no autorizado a la computadora cliente. El protocolo le permite a un pirata ganar información acerca de la red y su configuración incluyendo los anfitriones y nombres de usuario. NIS no debe dejarse pasar a través del *firewall* hacia una red externa como Internet.

- **SMNP**. Protocolo de administración simple de redes (*Simple Network Management Protocol*). Este protocolo permite que un administrador de red maneje los recursos a través de un nodo remoto. Las instrucciones de este protocolo no debe permitirse que pasen a través del *firewall* desde Internet, ya que un pirata podría ganar la capacidad para manejar la red externamente, cambiar configuración, rescribir las políticas de seguridad, etc.
- **TFTP**. Protocolo de transferencia de archivos triviales (*Trivial File Transfer Protocol*). TFTP es utilizado para reiniciar una computadora desde otro punto en la red. TFTP opera en el puerto 69, una operación cotidiana sería que una computadora inicia una sesión TFTP con un servidor de arranque desde donde transfiere los archivos de sistema necesarios para arrancar. Este protocolo también puede usarse para transferir archivos a cualquier computadora en la red, su uso más común es transferir software para configuración en sistemas sin disco duro, tal como ruteadores. Este protocolo no debe permitirse pasar a través del *firewall* que protege la red de Internet, un atacante podría usar TFTP para tomar información importante, archivos de passwords o colocar puertas traseras o algún otro código dañino. Este servicio debe instalarse en una computadora o servidor que no tenga contacto con Internet o redes externas.
- **Windows X**. Xwindows es un ambiente grafico para el software de aplicación de usuario. Este ambiente soporta servicios distribuidos usando puertos TCP y esta diseñado para controlar y mostrar de manera remota procesos a través de la red. En este sistema existe el riesgo de que un proceso dañino tome control o vigile la pantalla, o los dispositivos de teclado y mouse. La necesidad de abrir muchos puertos le da a un intruso la oportunidad para usar un puerto abierto y comprometer un sistema confiable con una conexión vulnerable. Por sus características a Windows X no se le debe permitir el paso hacia afuera del *firewall*. Al usar este ambiente se recomienda usar un programa que vigile la detección de intrusos en la red, así como un antivirus con protección en tiempo real.
- **GOPHER**. Gopher es un sistema cliente-servidor diseñado para localizar y recuperar archivos o información desde servidores por toda Internet. Los tipos de datos recuperados pueden ser archivos de gráficos o texto, programas *script* y archivos binarios ejecutables. Si estos archivos son recuperados y ejecutados sin que el usuario lo analice es posible que se obtenga y ejecute código dañino (virus o caballos de Troya). Por esto se recomienda que al usar Gopher la información recuperada sea revisada con programas antivirus antes de ser ejecutada.
- **ICMP**. El protocolo de mensaje de control de Internet es utilizado para determinar la información de ruteo y el estado del anfitrión. Un paquete de redirección ICMP es utilizado para informar a un ruteador o computadora sobre "nuevas y mejores" rutas hacia un destino. Estos paquetes pueden ser falsificados para dar rutas falsas hacia un destino y permitir a un atacante entrar a un sistema. Otro paquete común de ICMP es conocido como mensaje inalcanzable. Este paquete señala problemas con una ruta a una dirección destino. Si se falsifica un mensaje de este tipo se puede causar la negación de acceso a otra red o anfitrión. Para proteger el sistema de esta vulnerabilidad se puede configurar el servidor de ruteo o el *firewall* para ignorar los mensajes inalcanzable ICMP. "PING" es un servicio ICMP el cual envía un paquete a un destino dado preguntando sí "¿esta vivo?", la dirección destino regresa una afirmación o un mensaje inalcanzable ICMP. Lo recomendable al usar este servicio es filtrar los paquetes ICMP y no permitirles el acceso a través del *firewall* que protege la red.
- **RPC**. Una llamada a procedimiento remoto (RPC) es similar a una llamada a procedimiento en C. La diferencia es que una RPC incluye una dirección IP remota y un puerto. El procedimiento es llamado en una computadora y ejecutado en otra. Estas llamadas a procedimiento y los puertos pueden ser usados por un pirata informático para obtener acceso no autorizado a los recursos e información sobre un sistema. La recomendación es que las llamadas remotas a procedimientos deben ser filtradas e impedirles el acceso a través del *firewall*. Aunque existe el problema de que algunas aplicaciones de Windows

requieren de RPC para seguir operando, por lo que se deben abrir numerosos puertos para apoyar la funcionalidad de RPC, causando numerosos y serios problemas de seguridad.

- **DNS**. El sistema de nombres de dominio (DNS) es un método jerárquico y distribuido de organizar el espacio de nombres en Internet, se encarga de darles nombre a las direcciones de IP. Utilizando este sistema, un host hace una petición con un datagrama de protocolo de usuario (UDP) a un servidor DNS. Las peticiones también pueden hacerse con TCP (en el puerto 53) y se les da el nombre de transferencias de zona. Las transferencias de zona pueden ser usadas por piratas para obtener listas de posibles blancos. Se recomienda que el acceso a este puerto sea permitido solo a servidores secundarios de dominio conocidos.
- **E-mail**. *Electronic mail* es una de las aplicaciones más usadas en Internet. Los mensajes son transportados utilizando un formato especifico para ellos junto con el protocolo de transporte para el correo simple (SMTP). Los mensajes de correo electrónico no ofrecen funciones de seguridad, pueden ser leídos, modificados y falsificados por un pirata que este posicionado en la red entre la fuente y el destino del mensaje. Lo recomendable para esta situación y agregar un mejor nivel de seguridad es aplicar un algoritmo de criptografía al mensaje antes de enviarlo, para garantizar la integridad del mensaje y autenticidad de su origen se utiliza la firma digital.
- **SMTP**. El protocolo de transporte para el correo simple (SMTP) es un protocolo en el nivel de aplicación utilizado para distribuir mensajes de correo electrónico entre computadoras. Este protocolo es muy simple y entiende solo mensajes y comandos basados en texto simple. SMTP no ofrece ningún método para verificar la fuente del mensaje o su integridad, en caso de utilizar este protocolo se recomienda usar en conjunto a un nivel mas alto el protocolo PEM. El uso de SMTP exige la utilización de un servidor de correo central. Este servidor de correo debe ser el único que tenga acceso a través del *firewall* hacia Internet.
- **PEM**. El correo de privacidad mejorada (PEM) es un conjunto de estándares para agregar seguridad al correo electrónico de Internet. Este conjunto de estándares describe un protocolo de seguridad que puede ser utilizado encima del SMTP o del protocolo ***Unix-to-Unix Copy Protocol*** (UUCP). PEM provee tres servicios de seguridad: integridad, autenticacion del origen, y confidencialidad. PEM define un algoritmo de encripción asimétrica para la administración de llaves y operaciones de firma digital, y un algoritmo de encripción simétrica para encripción del mensaje.
- **PGP**. El paquete de encripción de muy buena privacidad (PGP) hace uso de encripción por llave pública para proteger correo electrónico y archivos de datos. Permite la comunicación segura con desconocidos, sin necesidad de canales seguros para un intercambio de llaves. Da un servicio rápido, con un sofisticado manejo de llaves, firmas digitales, compresión de datos. PGP usa el algoritmo RSA para el manejo de llaves y firmas digitales, y usa el algoritmo IDEA para proveer de confidencialidad.
- **MIME**. Las extensiones multipropósito de correo de Internet (MIME) fueron creadas por la Fuerza de Tarea de Ingeniería de Internet (IETF) como una solución que le permite a los usuarios adjuntar objetos cuyo formato no es texto a los mensajes de Internet. Algunos de los programas de correo electrónico MIME le dan al usuario la opción de configurar el tipo de datos adjuntos que son aceptados, y como ser interpretados, siendo muy importante para evitar que ciertos datos adjuntos se ejecuten e interpreten de manera automática, así se evita que virus o gusanos se introduzcan en nuestro equipo por este medio.
- **HTTP**. El protocolo de transferencia de hipertexto (http) es un protocolo a nivel aplicación utilizado para acceder a la red de cobertura mundial (www). Este protocolo transfiere un bloque de información y una descripción del tipo de datos al programa cliente (Internet Explorer, Netscape Navigator, Lynx, Mosaic), y este se encarga de interpretar la información para presentarla al usuario de forma correcta. El recibir código ejecutable es una actividad normal con este protocolo, por lo que se debe cuidar el configurar los programas cliente para preguntar antes de ejecutar cualquier *script* o código y revisar con programas antivirus cualquier código ejecutable descargado. Algunos sitios en Internet

utilizan el protocolo https que es una versión segura del http, donde se agregan las cualidades del PEM sobre http para encriptar y autenticar el mensaje.

- **IPSec**. IPsec es el protocolo estándar para la aplicación de confidencialidad, autenticación e integridad en la capa del datagrama de IP. IPsec comprende la base para la interoperabilidad de "tuberías" aseguradas de terminal-a-terminal, túneles encapsulados y Redes Privadas Virtuales (VPNs). IPsec esta basado en el algoritmo Diffie-Hellman y el algoritmo RSA para el intercambio de llaves. Para la encripción simétrica, los algoritmos DES y Triple DES son utilizados. En situaciones donde mayor seguridad es requerida para encripción en IPsec, el algoritmo RC5 es utilizado comúnmente. Las capacidades de IP son aplicadas en la capa de IP y para otorgar sus servicios de seguridad utiliza los protocolos del ***encapsulating security payload*** y ***autentication header***. Se recomienda el uso de este protocolo si se esta utilizando la versión 4 del protocolo de Internet.
- **SSL**. Secure Socket Layer (SSL) provee una capa de seguridad entre TCP y las capas de protocolos de aplicación. SSL otorga integridad y confidencialidad para cualquier flujo de datos TCP y puede ser usado con otros protocolos de nivel aplicación como http, Telnet, etc. Después de habérsele hechos algunos cambios a SSL 3, se obtuvo TLS (Transport Layer Security). Los algoritmos que utiliza se pueden seleccionar de varios disponibles. Este protocolo puede utilizarse tanto en computadoras clientes como en servidores y se recomienda en gran medida su utilización cuando se quieran hacer transacciones con tarjetas de crédito o establecer conexiones aseguradas por Internet.

JAVA. Sun Microsystems desarrolló el concepto de ***applet***, un programa que corre dentro de un navegador de Internet. Este tipo de programas son descargados de la red de manera dinámica con la finalidad de que los navegadores puedan entender e interpretar nuevos tipos de información que aparecen en las páginas web. Tal extensibilidad le permite a los navegadores crecer y adaptarse a las nuevas necesidades, la descarga de código sin la participación directa o conocimiento tiene serias implicaciones de seguridad. Sun Microsystems diseño el subsistema JAVA para encarar los problemas de seguridad. Java consiste de un interprete para una maquina virtual, la cual es independiente del tipo de máquina por lo que un solo ***applet*** puede usarse con cualquier computadora. JAVA esta diseñado para encargarse de los problemas de seguridad protegiendo al navegador y al usuario de ataques. Sin embargo en sus primeras versiones aun pueden causarse negación de servicio, degradación de servicio, encubrir comunicaciones, modificaciones en el navegador, todo esto a causa de vulnerabilidades que presenta JAVA: Una ausencia de una política de seguridad bien definida, falta de un mecanismo de seguridad que sea siempre invocado, falta de un mecanismo de seguridad que sea a prueba de entradas, falta de defensa profunda, falta de una base confiable de computo. Sin embargo en nuevas versiones del mecanismo JAVA se han arreglado varios de estos problemas de seguridad al mismo tiempo que varios navegadores funcionan de manera más suave y ya consideran entre sus actualizaciones de seguridad la descarga de ***applets***. El uso de los exploradores depende en gran medida si el administrador del sistema permite que las computadores terminales de la red se pueden conectar a Internet y si él considera necesario que la información proveniente de páginas que utilicen información JAVA pueden atravesar el *firewall*. Una recomendación en este caso es controlar a través del *firewall* el acceso a las páginas si estas son confiables. Si el administrador tiene conocimientos en JAVA entonces él puede revisar el código que se descargue de las páginas web, aunque este puede ser un procedimiento tedioso y tardado, para ahorrar este esfuerzo simplemente se puede restringir el acceso a las páginas que se considere confiables, verificando continuamente su dirección IP. Se recomienda utilizar una versión nueva de los navegadores y seguirla actualizando, descargando actualizaciones de seguridad para los navegadores que se encuentran disponibles en Internet, ya que estos arreglan muchos de los problemas de seguridad causados por JAVA.

COPIAS DE RESPALDO. En las redes de computadoras deben hacerse copias de respaldo con frecuencia, debido a la gran cantidad de información que se maneja. Estas copias deben ser

hechas de los archivos mas importantes como las bases de datos que se comparten en la red y toda clase de archivos privados e importantes para el funcionamiento del sistema de cada computadora. Es recomendable un mantenimiento periódico de todas las copias de respaldo, las cuales serán útiles en la reinstalación del sistema en caso de que algún ataque informático cause daños irreparables en el sistema o por efecto de virus que borren archivos clave. Con estas copias de respaldo también se deben tomar ciertas precauciones de seguridad, por ejemplo, los respaldos deben guardarse de preferencia fuera de la red pero que estén fácilmente disponibles para emergencias; estas copias de respaldo deben ser hechas por el administrador del sistema o por el responsable de la seguridad en la red y para una mejor protección pueden ser encriptadas, sin embargo, hay que asegurarse de tener acceso rápido a los programas de desencripción.

DETECTORES DE INTRUSOS. En la configuración cuatro también podemos aplicar los detectores de intrusos. Los detectores de intrusos se clasifican de dos maneras: sistemas de detección de intrusos en redes (NIDS) y sistemas de detección de intrusos en *host* (HIDS), así que para la cuarta configuración de sistemas mostrada en este documento, será útil la capacidad para proteger redes. El área de la detección de intrusos se encarga de informar de los eventos que puedan ser considerados como parte de un intento de intrusión en el sistema. Un efectivo sistema de detección de intrusos (IDS) debe ser capaz de diferenciar entre un acceso permitido por alguna aplicación que pone en marcha otros programas y uno no autorizado que busca vulnerar, robar o dejar inhabilitado ciertos recursos. Esta característica es especialmente importante si se tiene en mente que una red con conexión a una red extema (Internet) tendrá varios programas que envían información y reciben información por la puerta a Internet, y esto se presta para accesos de atacantes. El sistema de detección de intrusos también debe proporcionar conocimiento al administrador de red o responsable de la seguridad sobre la puesta en marcha de un ataque antes de que tenga éxito.

Generalmente la técnica para detectar intrusiones es el análisis por reconocimiento de patrones de ataques conocidos. En este aspecto son parecidos a los detectores de virus, ya que buscan detectar patrones para diferenciar un ataque de algo que no lo es. Para esto se basan en la búsqueda de anomalías, para llegar a ellas se emplean las técnicas de: clasificacion, episodios frecuentes, asociación de valores y análisis adaptivos. Para un desempeño eficaz se debe instalar primero el detector en modo de "aprendizaje" para analizar la información del transito y operaciones normales en la red y sus aplicaciones, posteriormente se dispone el detector en modo "analizar" para que este pendiente y busque actividad irregular, por ejemplo: el trafico fuera de horas de oficina, envío de información hacia el exterior de la red, recepción de información hacia el interior, etc. Sin embargo se debe mencionar que no son técnicas sin fallas, se pueden presentar **falsos positivos** los cuales son alarmas de intrusiones cuando no existe tal, los **falsos negativos** son intrusiones que pasan desapercibidas. Los NIDS analizan todo el trafico de la red, examina los paquetes para buscar opciones no permitidas. El análisis en toda la red lo hacen mediante el uso de agentes sensores, que reportan las alarmas hacia una consola central. La mayoría de los NIDS no necesitan software adicional en los servidores, sin embargo tienen la desventaja de un alto número de falsos positivos y que con los reportes de los agentes incrementan el trafico en la red, y tienen dificultades para detectar ataques encriptados. Los detectores de intrusos son parecidos a los *firewalls* en que debe elegirse muy bien la posición en la red donde se colocara, de manera que tenga acceso a los recursos de esa área. Cada nueva versión de los detectores viene mejor preparada para las nuevas tecnologías y ahora podemos encontrar que tienen la capacidad de trabajar en redes de transito elevado con velocidades de Gigabit y conexiones de banda ancha a Internet, e inmunidad a las técnicas *stealth* que utilizan los piratas. Los detectores de intrusos pueden configurarse para que sean activos o pasivos. Si se designa como activo, el IDS responde ante una actividad ilegal de forma activa sacando al usuario de la red, si se designa como pasivo el programa detectara la actividad inusual, genera la alerta y un registro de ella.

Algunos ejemplos de herramientas de detección son: ***Omniguard, Cisco Secure IDS, RealSecure, Kane Security Analyst, Centras***. Los IDS deben adaptarse a los recursos de la

empresa o lugar donde se tenga la red que se quiere proteger y estos deben ser incluidos en las políticas de seguridad de la empresa.

CONTROL DE ACCESO Y AUTENTICACIÓN. Una red de computadoras LAN con conexión a Internet permite compartir archivos, servicios de impresión, y el almacenamiento de archivos. Como estos servicios no están disponibles a un solo usuario, es necesario su control. Es por ello que debemos proteger nuestra red contra accesos no autorizados en la red local. En una configuración de sistemas informáticos tal como la red se tienen aplicaciones corriendo en las terminales y al mismo tiempo enlazadas con otras y con salida y entrada de datos de Internet, por ello el control de acceso es el responsable de la autenticación de los usuarios del sistema compartido por la red. Y en este caso el responsable de la implementación del control de acceso es el administrador del sistema. Las recomendaciones son muy parecidas a las de las configuraciones uno, dos y tres:

- La implementación de bitácoras de acceso a la computadora en conjunto con un proceso de autenticación de usuario por medio de passwords, así, en la bitácora quedara asentado quien tuvo acceso a la terminal, el día y la hora y las operaciones que llevo a cabo en ella.
- Dentro de los programas de acceso se puede implementar la característica de que los usuarios solo podrán acceder a la terminal a cierta hora del día, teniendo un control total sobre quien esta usando cada maquina a determinada hora.

El control de acceso considerara el proceso de autenticación de usuarios por medio de medidas de software, es decir, por medio del uso de passwords. La autenticación de los usuarios debe considerar varias situaciones: usuarios que escriban mal su password, mal funcionamiento del teclado, etc. Para el caso de uso de passwords ciertas medidas pueden ser programadas por dentro del programa controlador de accesos:

- Implementar un pequeño retardo en el proceso de verificación de 5 a 10 segundos. Para un usuario normal este proceso presentara un mínimo de molestia, sin embargo, para un posible perpetrador de robo de información y acceso no autorizado que use programas de ataque por búsqueda en diccionario, este retardo en cada intento de introducción de password hará que el ataque sea infeasible.
- Determinar el número de intentos de passwords equivocados que puede hacer un usuario. En caso de que sea muy importante para el negocio mantener ladrones fuera del sistema, con tres oportunidades basta. Si se dan las tres entradas equivocadas la cuenta del usuario debe ser dada de baja y solo el encargado de seguridad puede volverla a habilitar. Esto facilita la identificación de cuentas que están bajo ataque o en peligro por perpetradores.
- Programar el sistema para que obligue a los usuarios a cambiar de password periódicamente. Para evitar el reuso de passwords algunos sistemas de control de acceso rechazan cualquier password que haya sido usada recientemente.

Una técnica muy recomendable en el uso de passwords es utilizar las llamadas passwords de "uso único" (*one-time password*). Estas cambian cada vez que son usadas. En las passwords de uso único al usuario se le asigna no una frase, sino una función matemática. Aquí el sistema da un argumento para la función y el usuario debe introducir el valor resultante. Un sistema que utilice esta técnica es llamado desafío-respuesta (*challenge-response*) porque el sistema le presenta al usuario un desafío y determina la autenticidad del usuario por su respuesta. Las funciones que se definen para las password de uso único pueden llegar a ser muy complejas, por ejemplo: $f(E(x))=E(D(E(x))+1)$ en donde la computadora envía un valor encriptado $E(x)$ y el usuario debe desencriptar el valor, aplicar la función aritmética $+1$ y encriptar el nuevo resultado para enviarlo de regreso al sistema. Los passwords de uso único son muy seguros ya que si descubren uno este es inútil para volver a entrar al sistema.

Estas recomendaciones son hechas pensando en que solo se debe desconfiar del usuario, pero existe el caso en que el sistema de la terminal ya haya sido comprometido, es muy sencillo crear un programa que muestre o simule el símbolo del sistema y los espacios para el ID del usuario y el password, capture la información escrita y la guarde. En este tipo de ataque el

perpetrador escribe el programa, lo coloca en la terminal, espera que alguien escriba su password y se aleja sin que nadie se de cuenta. Las recomendaciones para evitar este tipo de ataque son:

- Asegurarse de siempre reiniciar la ruta al sistema. En algunos sistemas el presionar la tecla BREAK detiene los procesos que se realizan, o proceder al apagado y encendido de la terminal.
- Para asegurarse que la computadora esta corriendo el sistema que se desea, se puede programar el control de acceso para que antes de introducir password o datos confidenciales, muestre la fecha de la ultima vez que el usuario entró al sistema. Si se desea un mayor nivel de seguridad se puede encriptar el mensaje con la fecha, y el usuario se encargara de desencriptar y verificar la información, si es correcta el usuario encripta la fecha y el password para garantizar que un intruso no haya interceptado el password. Estas encripciones y desencripciones pueden ser hechas con algoritmos del tipo DES.

Si la red local tiene varios servidores de información, se pueden usar los programas de control de acceso para restringir el trafico entre los servidores. Esto se debe especificar en las políticas de manejo de la red local, de modo que el transito de información trivial entre servidores debe ser restringido.

Varias compañías de software se dedican a desarrollar sistemas de control de acceso. Estos paquetes proveen de autenticación de usuario, limitación en los accesos y bitácora de registro, por ello es recomendable la utilización de estos programas.

El administrador de la red debe tener en consideración algunas situaciones, como por ejemplo:

- Evitar otorgar permisos de escritura a usuarios que solo necesitan permisos para leer archivos importantes
- Implementar un *checksum* encriptado para información delicada.

KERBEROS. LA configuración cuatro considera una red con conexión a Internet, por tanto igual que en la configuración tres se puede considerar la tecnología de un sistema Kerberos para la autenticación de los usuarios dentro de una red ya protegida por un *firewall*. Para esto hace uso de la encripción por llave pública y llave privada. Kerberos es utilizado para procesos entre sistemas inteligentes tales como, tareas de servidor a cliente, o entre usuarios de las computadoras en la red. Kerberos se basa en tener un servidor central el cual provee de "boletos" autenticados para las aplicaciones que los requieran. El "boleto" es una estructura de datos autenticados definiendo a un usuario y un servicio que el usuario esta permitido a utilizar, contiene valores de tiempo e información de control.

Para empezar, primero se tiene que iniciar una sesión con el servidor de Kerberos, la estación de trabajo del usuario envía la identificación del usuario al servidor cuando este introduce su identidad. El servidor de Kerberos se encarga de verificar que el usuario este autorizado y envía dos mensajes: A la estacion de trabajo del usuario le envía una llave de sesion S_G para que la utilice en la comunicación con otro servidor que otorga los "boletos" y un boleto T_G para el servidor de boletos, tipicamente S_G esta encriptado con el password del usuario $E(S_G+T_G,pw)^2$. El otro mensaje que envía Kerberos es al servidor de boletos, envía una copia de S_G y de la identidad del usuario, encriptado con una llave compartida entre Kerberos y el servidor de boletos. Con este intercambio finalizado, si la estación de trabajo del usuario es capaz de desencriptar $E(S_G+T_G,pw)^2$ con el password del usuario, entonces la terminal y el usuario se han autenticado. Con la llave de sesión S_G el usuario puede solicitar boletos para accesar archivos o recursos y el servidor de boletos otorgara los permisos y derechos para el nivel de este usuario.

Kerberos fue diseñado para poder resistir ataques y evitar los accesos no controlados ya que:

- Los passwords son almacenados en el servidor de Kerberos y no en la estación de trabajo y el password del usuario tampoco ha sido enviado por la red.
- Cada petición de acceso es mediada por el servidor de boletos, el cual conoce la identidad de quien hace la petición por el proceso de autenticación que hizo con Kerberos.

- Cada boleto esta limitado a tener validez solo durante determinado tiempo, así, en caso de presentarse un ataque de criptoanálisis por fuerza bruta no hay tiempo suficiente para completar el ataque.
- Kerberos necesita usar un reloj universal ya que cada petición del usuario al servidor queda grabada con la hora en que se hizo. Cuando llega una petición al servidor, este compara el tiempo en que se hizo con el tiempo actual y completa la petición si el tiempo de la petición es razonablemente cercano al actual. Eso previene los ataques por "replay" porque la presentación del boleto del atacante se retrasa mucho.
- La autenticación mutua permite que el servidor otorgue un canal único al usuario, de manera que el usuario no necesite encriptar las comunicaciones en ese canal. Con menos información que encriptar se ahorra tiempo en las transferencias.
- Kerberos necesita para su operación un servidor dedicado para la utilización de sus estructuras que funcione en conjunto con el servidor otorgador de boletos y de servicios. Estos servidores estarán colocados dentro de la red y detrás del *firewall* que cubre la conexión a Internet.

CONTROL DE TRAFICO. En la configuración cuatro se puede aplicar la técnica de control de trafico. Al tener una red de computadoras con mucha información viajando entre ellas, el trafico se convierte en blanco de ataques de análisis. El análisis de trafico no es tan común como otros tipos de amenazas informáticas porque pocos atacantes están dispuestos a analizar todo el trafico de la red y que existen técnicas simples contra este análisis.

Como un interceptor ilegal puede revisar todos los bloques de mensajes que pasan en la red y conocer quien esta en comunicación continua, él se da cuenta cuando el trafico en cierta dirección aumenta con lo que puede adivinar alguna situación especial. El procedimiento simple es que para evitar un notorio aumento de trafico entre ciertas terminales, se introducen mensajes "sin uso" en las rutas con poco flujo. El lado negativo de esta técnica es que agrega carga a la red y el servicio a los usuarios puede degradarse.

Otro tipo de ataque es el establecer un canal encubierto en una red generando trafico, incluso trafico "sin uso". En esta técnica se representa un 1 binario con un mensaje hacia un nodo, y un 0 binario ya sea por la ausencia de mensaje o un mensaje enviado hacia otro nodo. Esta incursión en la red no requiere participación activa del intruso. Además de que este trafico puede parecer normal si esta dirigido hacia una terminal razonable, por ejemplo hacia un sistema de archivos. Este tipo de trafico puede permitir una enorme cantidad de información robada. Si en la organización o negocio necesitan un completo confinamiento de la red, el canal encubierto debe ser puesto fuera de circulación. Para ello hay dos técnicas: la introduccion de trafico y el control de ruteo. Estas técnicas de control de trafico son para evitar el robo de información de tipo interno, es decir que los cuidados del trafico son dentro de la red y debe funcionar en concordancia con el *firewall*, para tener un control completo de la información que sale hacia Internet.

La **introducción de tráfico** la acción llevada a cabo por el administrador de la red para introducir ruido entre los pares de terminales comunicándose. Este ruido es generado en forma de mensajes "sin uso" de manera aleatoria sin seguir ningún patrón, frecuencia, fuente o destino. Con este ruido, se espera que se distorsione el flujo de información en el canal encubierto. Las terminales legales deben ser capaces de reconocer los mensajes falsos para que no interfieran con la comunicación del usuario legitimo. El administrador de red no necesita participar en el trafico de la red mas que para generar mensajes de ruido periódicamente.

Para controlar los canales encubiertos, el administrador de la red puede ejercer un **control activo de ruteo** en la red. Por ejemplo, si el canal encubierto fuera 1 para el mensaje de A a B y 0 para el mensaje de A a C, el administrador puede tratar de redirigir los mensajes, haciendo un nuevo ruteo de los mensajes enviados de A a C para que vayan de A a B y después a C. De este modo, un mensaje A-C (0) será convertido a un mensaje A-B (1) seguido de un mensaje B-C (sin valor). Si la red maneja algún protocolo para detectar los mensajes perdidos, el administrador puede periódicamente borrar o desviar mensajes. Así, B se dará cuenta hasta mucho después de que un mensaje de A no fue recibido. Si esto pasa, B pedirá una retransmisión del mensaje, la

repetición del mensaje no afectara la comunicación normal. El flujo del canal encubierto será afectado porque otros mensajes ya pueden haberse transmitido, y este mensaje que representa un bit será transmitido fuera de secuencia. El administrador también puede retrasar los mensajes periódicamente. Con ello es posible que se destruya la sincronización entre la fuente y el intruso sin afectar de manera seria el trafico legitimo. Este tipo de control es muy efectivo si el canal depende del momento de llegada de mensajes.

Estos controles de trafico dependen de un administrador de red activo que pueda efectuar acciones en la red para destruir canales y afectar el trafico.[29]

CONTROLES DE HARDWARE

BIOS. Para la configuración cuatro de los sistemas de computación analizados aquí, las recomendaciones de seguridad serán iguales a las versiones anteriores. Es decir, la puesta a punto de la seguridad del BIOS ya que esto nos permite proteger las computadoras que comprenden la red durante el arranque. Esto se hace de la misma manera que para las configuraciones uno, dos, y tres. En el BIOS se selecciona que el sistema arranque primero desde disco duro y se pone un password para evitar cambios de esta secuencia o que alguien tenga acceso a la terminal.

En caso de que se use el sistema operativo LINUX, se puede utilizar el Linux Loader (LILO) para ceder el arranque del sistema, y superar el problema del cambio de jumper del BIOS. A LILO también se le agrega un password para evitar acceso o el cambio al estado inicial 1 donde se evita la autenticación del usuario por medio de password, esto se hace en el archivo ***/etc/lilo.con.*** Todos estos cambios en el BIOS o en el LILO se deben hacer en cada computadora que componga la LAN, de lo contrario, el sistema estará abierto a ataques. El administrador de la red o de la seguridad sería la persona más indicada para realizar esto.

SMARTCARDS. Las mismas recomendaciones se hacen en cuanto a las smartcards (tarjetas inteligentes), que generan cada determinado tiempo un password que permite el acceso hacia las áreas de la información critica que contiene la PC. Si no se tiene, el acceso es prácticamente imposible ya que el password que genera esta formado por letras y números de distinta longitud y obliga a ataques por fuerza bruta. Muchos negocios utilizan técnicas de autenticación biométrica en conjunto con smartcards; las técnicas biométricas miden alguna característica física única del usuario, tal como el patrón de la voz, de cara, el orden de los vasos sanguíneos de la cornea y las huellas digitales. Tradicionalmente, las representaciones digitales de las características biométricas ocupan un espacio entre 100 y 600 bytes y por ello se pueden acomodar en una smartcard. Los pasos característicos de una autenticación de usuario por medio de smartcard y medidas biométricas son los siguientes:

1. Insertar la smartcard en el lector, esta contiene las llaves criptográficas y los datos correspondientes a la huella digital del usuario.
2. Se introduce el número de identificación privada (PIN), así, se libera la representación electrónica de la huella digital.
3. Ahora se coloca el dedo en el escáner, esta huella es comparada con la guardada en la smartcard.
4. Si la comparación es positiva, los datos de la huella en la smartcard son convertidos a un valor numérico y se combinan con el PIN de la smartcard para formar una llave de encripción simétrica la cual desencripta la llave privada.
5. Un número aleatorio es generado por la computadora donde se conecta la smartcard, este número es transferido a la smartcard.
6. La llave privada en la smartcard es usada para encriptar el número aleatorio y mandarlo de vuelta a la computadora.
7. La computadora verifica que una llave pública certificada obtenida de algún directorio en red desencripte el número aleatorio y verifica que este sea el mismo que se envió originalmente a la smartcard.

Este proceso se encarga de autentificar de manera irrefutable al usuario de la smartcard. Cada usuario con acceso a estas computadoras debe de contar con su propia smartcard. Aquí, el administrador de la red quien estaría a cargo de la actualización y entrega de smartcards.

PUERTOS INFRARROJOS. En la cuarta configuración de sistemas informáticos se pueden aplicar los mismos métodos para proteger los puertos infrarrojos. Las computadoras conectadas en red y a Internet tienen iguales vulnerabilidades a nivel hardware que las máquinas de configuraciones anteriores: riesgo de sobreflujo del buffer y reinicio del sistema, copiado de archivos sin autorización e intentos de acceso. Para evitarlas, las medidas son las siguientes:

- Descargar los parches y actualizaciones que cubran esta vulnerabilidad y que ya están disponibles
- Hay que deshabilitar los dispositivos infrarrojos si no están en uso, no basta con deshabilitar la comunicación, sino que hay que deshabilitar todo el dispositivo utilizando el programa Administrador de Dispositivos
- Asegurarse que los puertos infrarrojos tienen bloqueada la línea de vista

También se puede colocar cinta opaca sobre el puerto aunque esto solo servirá si el oponente no tiene acceso a la máquina. Estas precauciones deben tomarse en cada una de las máquinas de la red que contengan puertos infrarrojos.

POLÍTICAS

Esta configuración de sistemas informáticos consiste en una red de computadoras conectadas a Internet. Es conveniente que antes de enunciar políticas dentro del negocio o compañía se definan los lineamientos de uso, hacer un análisis de riesgos en el sistema y establecer una estructura para el equipo de seguridad. Los lineamientos de políticas deben encargarse de contestar las preguntas: ¿A QUIEN se le permite acceso? ¿A QUE recursos? y ¿COMO se regula el acceso?. Las políticas también deben especificar: las metas en seguridad de la organización, quien tiene la responsabilidad de la seguridad, y el compromiso de la organización con la seguridad. En esta configuración se pueden imponer las siguientes políticas, aunque esto depende de las necesidades de seguridad del negocio ya que las políticas se pueden hacer más restrictivas o más libres.

- Especificar dentro de la compañía que acciones se consideran como ataques a la seguridad y las acciones a implementarse cuando se detecte uno.
- Especificar el nivel de autoridad que tendrá el equipo de seguridad para poder enfrentar situaciones de ruptura de seguridad y que tenga la capacidad de apagar todos los equipos afectados o el aislamiento de ciertos recursos.
- El administrador de la red o el equipo de seguridad cada determinado tiempo deberá hacer un análisis de riesgos y ver que nivel de riesgos le corresponde a cada dispositivo del sistema, ya sea las computadoras de la red, el equipo de autenticación, el quipo de red, etc.
- El administrador de la red o equipo de seguridad deberán efectuar auditorias en la red con los programas correspondientes para conocer todas las vulnerabilidades de la red y así trabajar en su solución.
- El administrador de la red o equipo de seguridad se encargan de buscar en Internet los parches necesarios para la corrección de vulnerabilidades que existen en el sistema operativo que se este utilizando en cada computadora de la red.
- El administrador de red entregara cada semana a los usuarios de las terminales un nuevo password para cada aplicación, inicio del sistema, o conexión a Internet.
- El equipo de seguridad deberá asignar un nivel de riesgo a cada uno de los siguientes: dispositivos de la red, dispositivos de distribución de redes, dispositivos de monitoreos de redes, sistemas de e-mail, o servidores de archivos en red.
- Para no arriesgar la información confidencial, esta debe ser almacenada en forma encriptada.

- Los monitores y las impresoras deberán colocarse en lugares donde la visibilidad de su información le sea imposible a otras personas que transiten por esos lugares.
- Prohibirle a los usuarios generales el descargar programas de procedencia dudosa de Internet ya que estos podrían traer escondido código de virus o de programas trojan.
- La firma de cláusulas explicitas dentro de los contratos de los trabajadores en donde acepten el no revelar información a competidores. Esto permitirá emprender acción legal contra alguno de los empleados o competidores si se llegara a revelar información clasificada.

Las políticas de seguridad son reglas que nos dictan como conservar la seguridad y las acciones a tomar en caso de una ruptura a la seguridad e incursión dentro de la maquina que queremos proteger.

CONTROLES FÍSICOS

AUTENTICACIÓN BIOMÉTRICA. La configuración cuatro consiste en una red de computadoras conectadas a Internet, aquí también podemos utilizar las técnicas biométricas para evitar el acceso a computadoras o a los edificios y oficinas donde se encuentran las computadoras conectadas a la red. Se pueden emplear los siguientes métodos de protección:

- Revisión de retina.
- Las técnicas de reconocimiento de voz y de firma de usuario, aunque estas no son biométricas.
- Técnicas de autenticación de rostro, mano o huellas digitales.

Tal y como se vio en la configuración tres, antes de aplicar estas técnicas hay que investigar si todas las computadoras se encuentran en la misma oficina o en oficinas separadas, y si será necesario instalar el equipo para el control de acceso a cada una de estas máquinas u oficinas y al cuarto donde se encuentre el administrador de la red y el servidor de Internet. El uso y aplicación de estas técnicas depende de evaluar previamente varios factores: nivel de seguridad que se necesite, costo y tiempo de implementación, aceptación de los usuarios y confiabilidad.

- Nivel de seguridad. El reconocimiento de voz y de firma son técnicas aceptables cuando se habla de usos no relacionados con autorización de acceso a la PC, sin embargo son útiles para la autenticación de usuarios de la red o de la PC. Las técnicas biométricas que identifican características físicas son más confiables y otorgan un nivel mayor de seguridad.
- Costo y tiempo de implementación. Cuando se desea implementar un sistema de autenticación biométrica de usuario, se debe de hacer en conjunto con el proveedor de computadoras y tomar en cuenta que hay que buscar e instalar el software y hardware compatible con la PC para autenticación (cámaras, lectores, scanners), el software y hardware necesarios para mantener la base de datos de usuarios, el tiempo que se lleva integrar el hardware de autenticación en el ambiente de trabajo, el entrenamiento del staff para manejar el nuevo sistema, el entrenamiento de los usuarios con el nuevo protocolo de autenticación y la actualización continua de las bases de datos.
- Aceptación de usuarios. Los usuarios generalmente aceptan las técnicas que son menos intrusivas o gorrosas, tales como identificación de huellas, rostro o mano. Aquí es responsabilidad de la organización el entrenar a los empleados para que se familiaricen con los nuevos requerimientos antes de que el sistema sea implementado.
- Confiabilidad. La revisión de retina e identificación de iris son altamente eficientes para identificar individuos, sin embrago, son muy costosas y la mayor parte de los negocios no necesitan este nivel de confiabilidad. Técnicas de autenticación de huellas, mano, y rostro ofrecen buena confiabilidad y requieren una menor inversión en equipo de revisión. Los cambios físicos tales como cortadas, cicatrices y el envejecimiento pueden afectar la identificación, sin embargo las bases de datos se pueden actualizar.

Existen dos términos que describen la funcionalidad de las técnicas biométricas: la razón de falsa aceptación (*False Aceptance Rate*, FAR) el cual describe la probabilidad de que un intruso sea aceptado con una medida que no le pertenece de un usuario enrolado. La razón de rechazo

falso (*False Rejection Rate*, FRR) es la probabilidad con que un usuario enrolado sea rechazado. Se considera que un buen equipo biométrico tiene un bajo FRR y FAR. Casi siempre hay un intercambio entre seguridad y conveniencia, en los sistemas biométricos mientras más seguro el sistema (mas bajo FAR) es más inconveniente para el usuario, ya que ocurren más rechazos falsos. Similarmente, mientras más conveniente sea el sistema, menos seguridad tiene. Los sistemas biométricos le permiten al usuario elegir entre un amplio rango de niveles de FAR/FRR.

Tomando en cuenta que puede haber ocasiones extremas en donde se utilice un dedo cortado de la mano o dedos falsos. Algunos diseñadores de equipo miden el calor del dedo en el escáner, otros miden su conductividad para evitar casos donde se modifiquen las huellas con silicón. La solución más adecuada es por medio de la medición **espectroscópica** de la cantidad de hemoglobina oxigenada en la sangre, ya que es imposible de pasar con dedos artificiales y los resultados de esta prueba son muy distintos para dedos vivos y dedos cortados.

En esta cuarta configuración también se pueden presentar muchos gastos, ya que quizá sea necesario proteger cada una de las computadoras y todo depende del tamaño de la red que puede ser de unas cuantas computadoras hasta varias decenas.

HERRAMIENTAS Y MEDIDAS FÍSICAS. Consideramos también en los controles físicos las estrategias y herramientas que ayudan a impedir los incidentes de robo o perdida de equipo de computo. En esta configuración tenemos una red de computadoras con conexión a Internet, así que las medidas de seguridad física que se recomiendan son:

- Designar un oficial de seguridad departamental, quien reportara rupturas en la seguridad y actos ilegales. Además será el responsable de implementar, coordinar, mantener y monitorear un programa de seguridad departamental.
- Debe restringirse el acceso a los gabinetes y closet donde se encuentran el cableado de las conexiones, los servidores de archivos, servidores de Internet y ruteadores.
- Para protección del servidor pueden usarse candados de tapas, las cuales son a prueba de abolladuras, y no contienen cables o adhesivos que dañen el equipo.
- Establecer puntos de recepción en las instalaciones, entre áreas funcionales o zonas seguras.
- Definir claramente los limites del acceso público en el edificio, por medio de señalamientos.
- Si es posible colocar todas las computadoras en una sola oficina para que solo se proteja una vía de acceso a ellas y así evitar grandes gastos en la aseguración de múltiples oficinas.
- Instalar puertas y ventanas que den entrada al edificio u oficina donde esta cada computadora de la red, las cuales deben contar con alarmas contra apertura o ruptura.
- Los cables de aseguramiento de computadoras son muy populares hoy en día y pueden ser otra opción en lugar del gabinete, así como placas de acero para aseguramiento de cada computadora de la red que la mantiene fija en su lugar.
- Vigilar frecuentemente que no haya algún cable superpuesto al cable que permite la conexión a la red de cada computadora de la red.
- Para evitar el acceso a las unidades de disco de las computadoras se emplean candados con llave, esto puede llevarse a cabo por los guardias o los mismos usuarios de las terminales al finalizar su jornada de trabajo.

Todas estas medidas son para prevenir el robo y destrucción, aunque se puede idear medidas más estrictas dependiendo de los requerimientos y tamaño de la empresa.

NIVEL DE SEGURIDAD

En la configuración cuatro se tiene una red de computadoras con conexión a Internet. Previo a la aplicación de las recomendaciones de seguridad, el nivel que tendría esta configuración seria de **1**.

Con pocos métodos de seguridad implementados se tiene una buena operatividad del sistema:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{1} = 1$$

Con las recomendaciones hechas en los apartados de **encripción, Controles de Software, Controles de Hardware, Políticas** y **Controles Físicos** se cubren las características descritas para la obtención del nivel **5** de seguridad.

Su nivel de operatividad esta determinado por la formula:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{5} = 0.2$$

El nivel de operatividad es el más bajo, obviamente esto depende de las necesidades en seguridad de la empresa o negocio. Si se desea un mayor nivel de operatividad, hay que buscar que servicios de seguridad no son necesarios para la operación del sistema de la empresa y descartarlos.

Tabla 4.5 - Niveles de Seguridad y Operatividad

Nivel de seguridad por default	**1**
Nivel de Operatividad por default	**1**
Nivel de Seguridad con recomendaciones	**5**
Nivel de Operatividad con recomendaciones	**0.2**

En la página 22 se definen las características de los niveles de seguridad del Orange Book, para tener una mejor referencia de la seguridad lograda con las recomendaciones de seguridad hechas para la configuración 4 se busca en que nivel del Orange Book quedaría y se puede ver que cubre los requisitos para lograr un nivel aproximado de **B3**. Esto es porque en las recomendaciones de seguridad se tocan los puntos de seguridad autenticada, diferencias para recursos de usuario y recursos de administrador, capacidad de auditorias, recomendaciones de encripción para comunicar la información entre terminales de la red, restricciones de acuerdo a usuarios y políticas, un control de usuarios del que es responsable el administrador del sistema, y protección por hardware también aplicada. El cubrir las características del nivel B2 depende de la etiquetación de objetos y eso puede variar en diferentes sistemas por la información y recursos que se manejen, así que bien puede ser cubierto y bien puede no serlo, depende del administrador. Así, el sistema muestra un nivel de seguridad muy elevado, solo por abajo del nivel A.

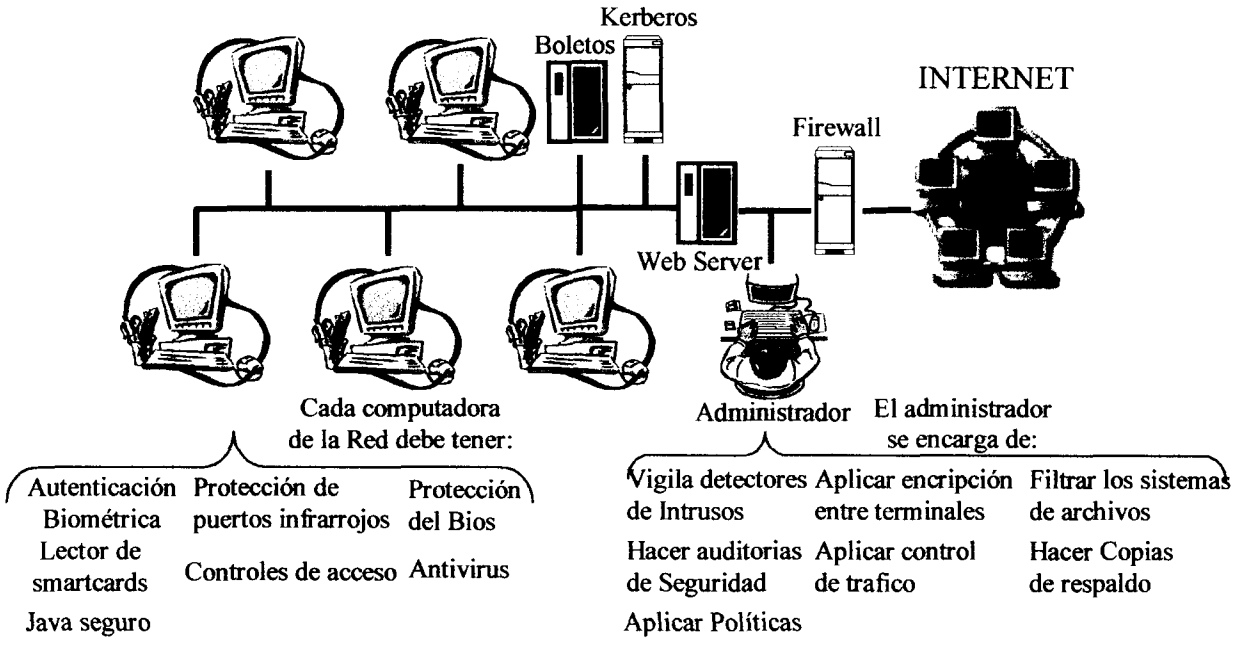


Figura 4.11 - Configuración segura

CONFIGURACIÓN 5 - Dos redes locales interconectadas por Internet

Otra configuración común dentro de las empresas y negocios que están actualizados y prestan sus servicios por medios computacionales es aquel en donde la empresa tiene una oficina matriz o central la cual se comunica con otra sucursal, esto implica que compartan bases de datos, recursos como impresoras o acceso a ciertas áreas del sistema.

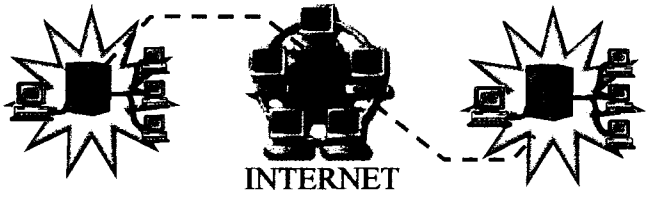


Figura 4.12 - Dos redes locales conectadas a Internet

En la configuración cinco, las recomendaciones de seguridad que se hacen son muy parecidas en varias secciones a las recomendaciones hechas para el caso de una red con conexión a Internet. Las características por default de seguridad de dos redes interconectadas a través de Internet consisten en: sistemas operativos sin parches de seguridad instalados, ningún tipo de autenticación de usuario o codificación para proteger archivos importantes o acceso a la red, servicios de red disponibles para personal no autorizado, ningún software de auditorias, falta de software o dispositivos que eviten las incursiones al sistema desde Internet, tampoco detectores de intrusos, además de tener casi todas las características de seguridad para operación en red de los sistemas operativos al mínimo por default. Muchos de los equipos de computo vienen de fabrica con programas antivirus instalados (aunque no necesariamente actualizados) y candados o elementos de seguridad física para cada computadora y servidor utilizado, como se trata de redes

es posible que varias computadoras estén en un solo lugar y se asegure el cuarto con llave, en esta configuración de dos redes si es necesaria la intervención de un administrador de red, quien, dependiendo de su pericia puede habilitar la autenticación y algunas políticas.

ENCRIPCIÓN

Las recomendaciones en las técnicas de encripción a utilizar son las mismas que aquellas que se hicieron en la configuración cuatro. Es dentro de la estructura de las Redes Privadas Virtuales donde se puede definir el tipo de encripción que se aplicara a los datos que circulan entre las redes.

CONTROLES DE SOFTWARE

En general, son las mismas recomendaciones que para la configuración cuatro, aunque se debe agregar las recomendaciones pertinentes para la utilización de las Redes Privadas Virtuales (VPN).

REDES PRIVADAS VIRTUALES. Mediante el uso de una Red Privada Virtual (VPN), una organización puede garantizar una red segura sobre un canal de comunicaciones que no es de confianza, como Internet, y al mismo tiempo ahorrar gastos al no tener que instalar líneas dedicadas y en métodos de acceso remoto.

Una VPN instalada correctamente puede proteger a un sistema de computadoras contra virus, intrusiones, espías corporativos y vulnerabilidades creadas por malas configuraciones, control de acceso deficiente, falta de administración del sistema o incluso de amenazas por "puertas traseras". Básicamente un arreglo de VPN debe proveer de encripción de la información en una red dinámica pública y a partir de esta puede otorgar otros servicios de autenticación, control de acceso y autorización.

La configuración cinco, es un sistema clásico para compañías con varias oficinas en donde dos redes locales se comunican a través de Internet. Normalmente se considera que la fuente y el destino de la comunicación entre ambas redes son confiables ya que pertenecen a la misma corporación, por lo que se puede elegir un modelo de VPN que favorezca el desempeño y no tanto a la seguridad. En una conexión así, hay un gran intercambio de información así que se debe elegir las características de configuración que permitan una alta velocidad y operación suave. Ambas redes locales si están conectadas a bases de datos centrales deben parecer que son parte de la misma red corporativa. Si la empresa se encuentra muy preocupada por evitar fugas de información intencional o accidental causada por los empleados internos, entonces se recomienda invertir en una solución de VPN que controle el flujo de información a un nivel de políticas especificas para usuario autenticado en lugar de hacerlo basándose en subredes confiables.

Las VPN más seguras son construidas utilizando la arquitectura dirigida en lugar del método de "tunelado". Las VPN dirigidas transmiten la información encriptada a un nivel mas elevado en la pila de protocolo de red que las VPN tuneleadas. Las VPN dirigidas actúan como servidores proxy, por lo que no abren ninguna conexión directa hacia las redes corporativas interiores, evitando así ataques de falsificación de direcciones. Las VPN dirigidas protegen las redes conectadas a ellas de fallas en otras redes, esto lo hacen ya que las VPN dirigidas no asumen una relación confiable bidireccional entre las dos redes, así, en caso de una ruptura en la seguridad con el modelo dirigido solo se pone en riesgo la red atacada, y las enlazadas permanecen seguras. Con el modo túnel de VPN, si una red es comprometida entonces todas las redes conectadas a ella también lo están. Las VPN de túnel, abren "túneles" a través de Internet y la información segura viaja por este túnel virtual, esta es una técnica que ofrece poca seguridad en el acceso a las redes mutuas. Si se van a llevar a cabo transacciones de negocios a través de redes públicas un simple túnel encriptado no ofrece suficiente seguridad, los negocios en línea y el comercio electrónico no están restringidos a transacciones de tarjetas de crédito. También engloba negociaciones complejas y colaboraciones en proyectos. En casos delicados, una VPN que incluya a una red local en comunicación con un compañero de negocios debe utilizar la encripción más compleja posible, además debe tener la capacidad de soportar múltiples métodos de autenticación

y encripción ya que los proveedores, y clientes y afiliados pueden tener infraestructuras variables de conectividad. En un escenario de negocios real, los administradores de seguridad de la red debe asegurarse de aplicar un filtro que controle el acceso a los recursos basándose en tantos parámetros como le sea posible y tener la capacidad de identificar al usuario individual, no solo su dirección de IP ya sea por medio de passwords, smartcards, o algún otro medio de autenticación. En un ambiente normal de oficina con la autenticación por password bastaría pero para otras aplicaciones más delicadas se necesitan medios más efectivos. En caso de que un usuario ya haya sido autenticado no debe dársele acceso completo a todos los recursos de la red, sino solo permisos específicos. Y además, tener en cuenta que conforme mas se acerque un usuario a la información más sensible, la seguridad también debe aumentar. Utilizando fuerte encripción, autenticación y métodos de control de acceso que funcionen dentro de la arquitectura de la VPN las compañías pueden alejar las amenazas de sus redes.

Cada corporación tiene sus propias necesidades de comunicación. Las pequeñas tiendas pueden solo requerir una manera segura de que sus empleados de viaje logren acceder remotamente a los recursos de la red corporativa. Mientras más grande sea la compañía, mayor será la necesidad de ella por compartir información entre sus empleados y oficinas sucursales. Las VPN que son implementadas en las capas dos y tres del modelo OSI deben mostrar un mejor rendimiento que aquellas en las capas superiores, y las VPN en las capas cinco y superiores deben dar una mayor seguridad.

Las VPN que utilizan el protocolo SOCKS están mejor capacitadas para compañías con altas necesidades de seguridad, conectividad cliente-servidor para soluciones de negocios. SOCKS es un estándar que funciona en la capa de sesión y por ello puede operar separado de protocolos de nivel más bajo o agregar valor a los protocolos de túnel de VPN que adolecen de capacidades de seguridad. El protocolo IPSec contiene las funcionalidades mas apropiadas para apoyar una VPN LAN-LAN. No requiere software de cliente, por lo que da atractivas soluciones a compañías que quieren intercambiar grandes cantidades de datos tan rápido como sea posible. Las VPN que utilizan PPTP y su variante L2TP, son mas apropiadas para acceso remoto, mientras que sea Windows la plataforma utilizada.

FIREWALLS. Un *firewall* nos permite controlar el acceso externo a elementos que se encuentran detrás del lugar donde esta ubicado el *firewall*, esto significa que podemos evitar ataques externos e intentos de envío de archivos no deseados. El firewall es un proceso que filtra el trafico entre su posición y la red exterior, esto lo hace al aplicar ciertas políticas, como puede ser evitar el acceso del exterior y alternativamente permitir el acceso al exterior de ciertas aplicaciones. Para la configuración cinco en donde se tienen dos redes locales conectadas a través de Internet se tiene que elegir una configuración de *firewall* que permita el transito de información rápido entre las dos redes y que funcione conjuntamente con la configuración de la VPN. Hay tres dispositivos que se entienden como firewall: *screening router, proxy firewall* y *guard*.

Para la situación de dos redes que desean compartir información a través de Internet el tipo de *firewall* más recomendable seria el *screening router*. Se debe de colocar uno a la entrada de cada red local, así, la compañía puede limitar la comunicación entre las redes. Así se dejaría salir de la red solo la información de ciertas aplicaciones con destino hacia la otra red, en el destino se puede configurar para solo recibir información para ciertas aplicaciones desde la otra red. El filtrado de información en los *firewall* se hace al revisar los encabezados de los paquetes de datos, un paquete es una subunidad de comunicación de unos cuantos cientos de bytes, un ruteador puede manejar miles de paquetes por segundo, por estas razones las reglas y políticas establecidas para el monitoreo de este *firewall* tienen que ser de rápida aplicación de modo que el trafico no sea haga lento. Los *screening routers* tienen la capacidad de verificar que los paquetes provengan de otras terminales en el interior de la red o que provengan de las otras redes de la compañía y que la dirección indicada en el campo de fuente del paquete no haya sido falsificada. Esta es una practica popular ya que permitiría enviar trafico exterior hacia dentro de la red, para evitarlo se configura el ruteador para que no permita la entrada a los paquetes externos que presumen de venir de una dirección interna.

PROGRAMAS ANTIVIRUS. Las recomendaciones para el manejo de los programas antivirus son iguales a las hechas para la configuración cuatro.

COPIAS DE RESPALDO. Recomendaciones para el manejo de copias de respaldo iguales que para la configuración cuatro.

JAVA. Las recomendaciones son básicamente iguales a las hechas en la configuración cuatro, todo depende de las libertades que se les quiera dar a los empleados y usuarios de la red para navegar en Internet.

KERBEROS. Las recomendaciones para el uso del sistema de autenticación Kerberos son las mismas que para la configuración cuatro, aplicándose en cada red local de la corporación que se desee proteger.

PROTOCOLOS Y SISTEMAS DE ARCHIVOS. Las recomendaciones que se hacen para el manejo de los protocolos y de los sistemas de archivos que funcionan en red, son las mismas que se hicieron para la configuración cuatro.

CONTROLES DE ACCESO Y AUTENTICACIÓN. Las recomendaciones en el área de controles de acceso son iguales que para la red presentada en la configuración cuatro, solo se debe considerar hacerlas para cada una de las redes y que debe funcionar de manera armónica con las opciones de configuración de la Red Privada Virtual. Este proceso de control y autenticación puede ser llevado a cabo por un programa separado o por los controles de la Red Privada Virtual.

DETECTORES DE INTRUSOS. Los detectores de intrusos son muy importantes para proteger la información contenida en las redes de computadoras, y en esta configuración también lo son. Deben de instalarse los elementos necesarios en cada red de la compañía para una seguridad completa sobre los intrusos detrás del *firewall*. En sí, las recomendaciones son las mismas que para la configuración cuatro.

CONTROLES DE HARDWARE

BIOS. Recomendaciones iguales a las expuestas en la configuración cuatro sobre el bios.

PUERTOS INFRARROJOS. Las recomendaciones son iguales a las dadas en la configuración cuatro para los puertos infrarrojos.

SMARTCARDS. Recomendaciones como las hechas en la configuración cuatro.

POLÍTICAS

El propósito principal de las políticas de seguridad es informar a los usuarios, el staff y los administradores de sus obligaciones para proteger la tecnología y la información. Las políticas deben especificar los mecanismos para atender estas obligaciones. Se puede considerar que usar un conjunto de herramientas de seguridad en ausencia de política de seguridad al menos implicada no tiene ningún sentido. Esta configuración de sistemas informáticos consiste en dos redes de computadoras conectadas entre sí por medio de Internet. A continuación se presenta una lista de políticas útiles para esta configuración, aunque no son las únicas a emitirse. Esta lista puede ampliarse y modificarse de acuerdo a las necesidades.

- Especificar dentro de la compañía que acciones se consideran como ataques a la seguridad y las acciones a implementarse cuando se detecte uno.
- El nivel de autoridad que tendrá el equipo de seguridad para poder enfrentar situaciones de ataques o incursiones dentro de la red por un atacante o hacker.

- Hacer un análisis de riesgos y ver que nivel de riesgos le corresponde a cada dispositivo del sistema.
- Los administradores o miembros del equipo de seguridad deben efectuar auditorias con los programas correspondientes para estar al día y conocer perfectamente las vulnerabilidades del sistema para trabajar en su solución.
- Para no arriesgar la información confidencial, esta debe ser almacenada en forma encriptada.
- Los monitores y las impresoras deberán colocarse en lugares donde la visibilidad de su información le sea imposible a otras personas que transiten por esos lugares.
- Los administradores de las redes y miembros del equipo de seguridad deben encargarse de buscar en Internet los parches necesarios para la corrección de vulnerabilidades que existen en el sistema operativo que se este utilizando en las computadoras de la red o en el servidor de la red.
- El administrador de seguridad cada semana entregara un nuevo password a los usuarios generales para cada aplicación, inicio del sistema, o inicio de sesión en la red debe de ser distinto.
- El equipo de seguridad tiene que asignar un nivel de riesgo a cada uno de los siguientes: dispositivos de la red, dispositivos de distribución de redes, dispositivos de monitoreos de redes, sistemas de e-mail, o servidores de archivos en red.
- El administrador de la red o los administradores de ambas redes periódicamente deben revisar el estado de la VPN, para verificar que no haya modificación de la información al ser transmitida por Internet.
- Nunca entrar a Internet si no esta activo el *firewall*, el programa antivirus o el programa detector de intrusiones.
- La firma de cláusulas explicitas dentro de los contratos de los trabajadores en donde acepten el no revelar información a competidores. Lo cual permitiría llevar a acabo acción legal si esto llega a pasar contra ellos o el competidor.

CONTROLES FÍSICOS

AUTENTICACIÓN BIOMÉTRICA. Para la configuración cinco las recomendaciones de controles físicos son las mismas que en las configuraciones tres y cuatro.

HERRAMIENTAS Y MEDIDAS FÍSICAS. Entre los controles físicos hay estrategias y herramientas que ayudan a impedir los incidentes de robo o perdida de equipo de computo. En esta configuración tenemos dos redes de computadoras interconectadas por Internet. Las medidas de seguridad que se recomiendan son similares a las configuraciones tres y cuatro en donde se protegen redes de computadoras. Las recomendaciones son:

- Designar un oficial de seguridad departamental, quien reportara rupturas en la seguridad y actos ilegales. Además será el responsable de implementar, coordinar, mantener y monitorear un programa de seguridad departamental.
- Monitorear el perímetro del edificio (o edificios ya que las redes pueden estar en lugares distintos) o las oficinas con cámaras de circuito cerrado.
- Para protección de los servidores pueden usarse candados de tapas, las cuales son a prueba de abolladuras, y no contienen cables o adhesivos que dañen el equipo.
- Debe restringirse el acceso a los gabinetes y closet donde se encuentran el cableado de las conexiones, los servidores de archivos, servidores de Internet y ruteadores.
- Definir claramente los limites del acceso público en los edificios, por medio de señalamientos.
- Si es posible colocar todas las computadoras pertenecientes a cada red en una sola oficina para que solo se proteja una vía de acceso a ellas y así evitar grandes gastos en la aseguración de múltiples oficinas.

- Instalar puertas y ventanas que den entrada al edificio u oficina donde está cada computadora de cada red, las cuales deben contar con alarmas contra apertura o ruptura.
- Los cables de aseguramiento de computadoras son muy populares hoy en día y pueden ser otra opción en lugar del gabinete, así como placas de acero para aseguramiento de cada computadora conectada a alguna de las redes que la mantiene fija en su lugar.
- Vigilar frecuentemente que no haya algún cable superpuesto al cable que permite la conexión a la red de cada computadora de ambas redes.
- Para evitar el acceso a las unidades de disco de las computadoras se emplean candados con llave, esto puede llevarse a cabo por los guardias o los mismos usuarios de las terminales al finalizar su jornada de trabajo.

Todas estas medidas son para prevenir el robo y destrucción, aunque se puede idear medidas más estrictas dependiendo de los requerimientos y tamaño de la empresa.

NIVEL DE SEGURIDAD

En la configuración cinco hay dos redes interconectadas por Internet. Previo a la aplicación de las recomendaciones de seguridad, el nivel que tendría esta configuración sería de **1**.

Con los métodos de seguridad implementados, la operatividad del sistema sería:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{1} = 1$$

Con las recomendaciones hechas en los apartados de **encripción, Controles de Software, Controles de Hardware, Políticas** y **Controles Físicos** se cubren las características descritas para la obtención del nivel **5** de seguridad.

Su nivel de operatividad esta determinado por la formula:

$$Operatividad = \frac{1}{Seguridad} = \frac{1}{5} = 0.2$$

El nivel de operatividad es el más bajo. Si se desea un mayor nivel de operatividad, hay que buscar que servicios de seguridad no son necesarios para la operación del sistema de la empresa y descartarlos.

Tabla 4.6 - Niveles de Seguridad y Operatividad

Nivel de seguridad por default	**1**
Nivel de Operatividad por default	**1**
Nivel de Seguridad con recomendaciones	**5**
Nivel de Operatividad con recomendaciones	**0.2**

De acuerdo a los niveles del Orange Book se puede ver que las recomendaciones de seguridad permiten que el sistema de la configuración cinco cubra los requisitos para lograr un nivel aproximado de **B3**. Las recomendaciones de seguridad tocan los puntos de seguridad autenticada, diferencias para recursos de usuario y recursos de administrador, capacidad de auditorias, recomendaciones de encripción para comunicar la información entre terminales de la red, un método de comunicación segura entre las redes para que compartan sus datos, restricciones de acuerdo a usuarios y políticas, un control de usuarios del que es responsable el

administrador del sistema, y protección por hardware también aplicada. El cubrir los requisitos del nivel B2 depende de la etiquetación de objetos y eso puede variar en diferentes sistemas por la información y recursos que se manejen, así que bien puede ser cubierto y bien puede no serlo, depende del administrador. Así, el sistema muestra un nivel de seguridad muy elevado, solo por abajo del nivel A.

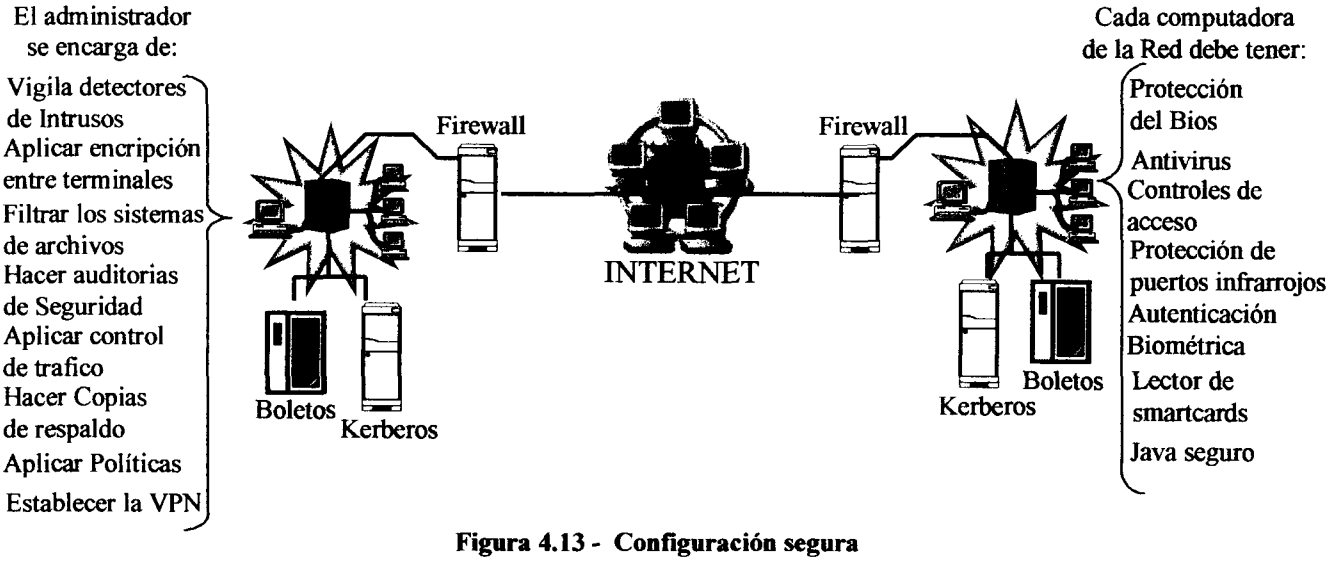


Figura 4.13 - Configuración segura

PRUEBAS DE ENCRIPCION

En este capitulo se analizan los resultados de pruebas realizadas con los algoritmos de llave pública y llave privada. Junto con esto se probó la transmisión de distintos archivos que habían sido previamente encriptados utilizando programas de encripción que hacen uso de algunos algoritmos de llave privada.

Las pruebas que se ejecutaran con los algoritmos de encripción no se encontraron en la bibliografía consultada. Con estas pruebas queremos probar las posibles aplicaciones en negocios donde se requiera la transmisión de texto o de algunos símbolos; los programas que generaran los archivos encriptados por medio de una llave privada son encontrados en Internet, se escogió utilizarlos por la facilidad con que los usuarios deseosos de privacidad pueden obtenerlos. Al tener un programa o algoritmo que se encargue de mandar de manera segura nuestra información, seguramente se presentará un incremento en las personas que utilicen las compras por Internet, la transferencia de dinero y la utilización de los números de tarjetas de crédito sin ningún problema. Muchas de estas transferencias son entre dos computadoras, por ello, las pruebas se harán también entre dos computadoras para poder apreciar cual es la exigencia sobre la red en cuanto a la transferencia de archivos encriptados. También busca probarse lo mencionado respecto a que los algoritmos de llave pública son poco útiles para encriptar mensajes por necesitar mas tiempo para la encripción que los algoritmos de llave privada. Los parámetros que se evalúan con la finalidad de poder apreciar si la encripción con cierto algoritmo realmente es conveniente son: tiempo de transmisión de archivos encriptados y tiempo de procesamiento para la encripción de archivos, observando además si el tamaño del archivo aumenta o disminuye. Al tener estos datos, se podrán comparar las características de velocidad y seguridad que cada algoritmo ofrece, esto

es muy útil porque permite apreciar las ventajas y desventajas de cada algoritmo analizados aquí, de esta forma los usuarios decidirán que algoritmo aplicar en sus sistemas de acuerdo a sus preferencias, adquiriendo la información necesaria para poder decidir si la característica de mayor resistencia a ataques en un archivo encriptado es más importante, mientras que otros pueden optar por tener una comunicación con una velocidad de transferencia constante y utilizar un algoritmo que otorgue cierta seguridad y no requiera demasiados recursos del sistema para la encripción.

Estructura del algoritmo de llave pública

En el caso de los experimentos aquí realizados con el algoritmo de llave pública, se debe hacer mención que se basa en operaciones hechas en MAPLE y la encripción es solamente sobre texto. El algoritmo que se usó esta basado en el RSA, el cual es uno de los algoritmos criptográficos más seguros. Las iniciales de RSA están tomadas de los nombres de los científicos que lo desarrollaron: Rivest, Shamir y Adleman. El sistema se basa en elevar exponencialmente el mensaje de un módulo que es muy grande. Sin embargo, la inversión o decodificación del mensaje no es una tarea simple ya que es necesario encontrar los factores primos del modulo lo cual es una tarea que lleva mucho tiempo si el número de dígitos es mayor de 200.

En 1977 se presento un desafío para decodificar un mensaje encriptado con el sistema RSA. El modulo de este mensaje era un número de 129 dígitos. Se estimaba que tomaría 40 cuatrillones de años descifrarlo por fuerza bruta, pero en solo 17 años los factores primos fueron calculados y el mensaje encontrado, esto gracias a los avances tecnológicos de los sistemas de computadoras. Por esto se sugiere que para un sistema seguro se deben de utilizar más de 129 dígitos para un módulo, siendo si es posible 200 o un número mayor.

La seguridad del sistema se basa en mantener privados dos números primos muy grandes. El producto de estos es el módulo. Posteriormente se hace una serie de operaciones que son implementadas de manera sencilla en el programa MAPLE.

Para comprender mejor el proceso de encripción se puede observar cómo es la estructura básica del algoritmo de encripción de llave pública implementado en MAPLE en la figura 4.14:

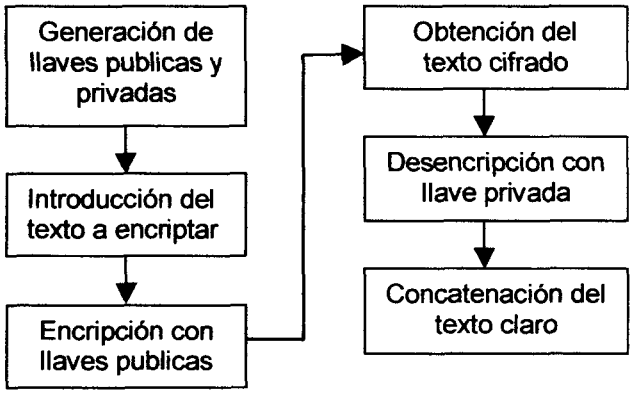
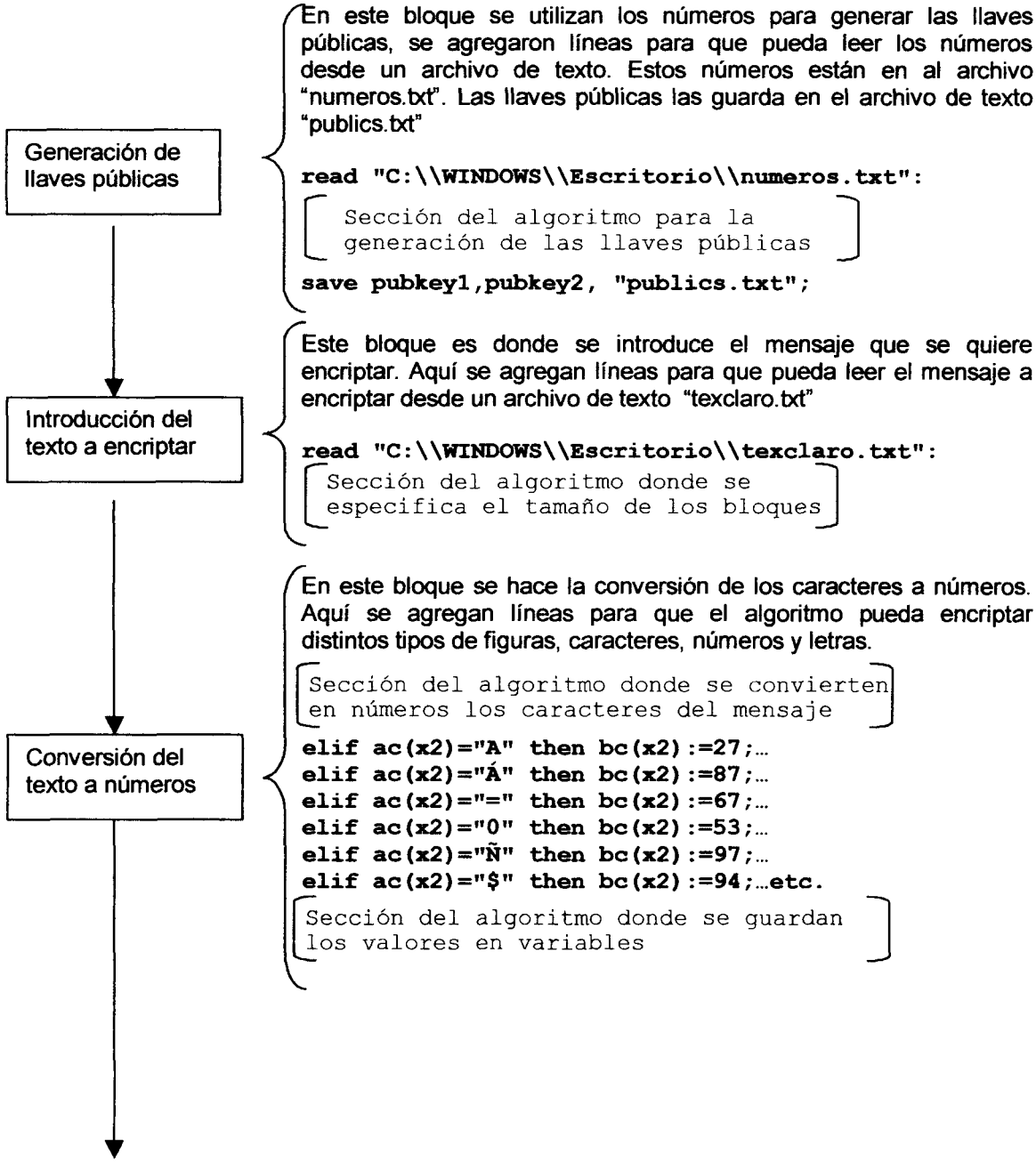
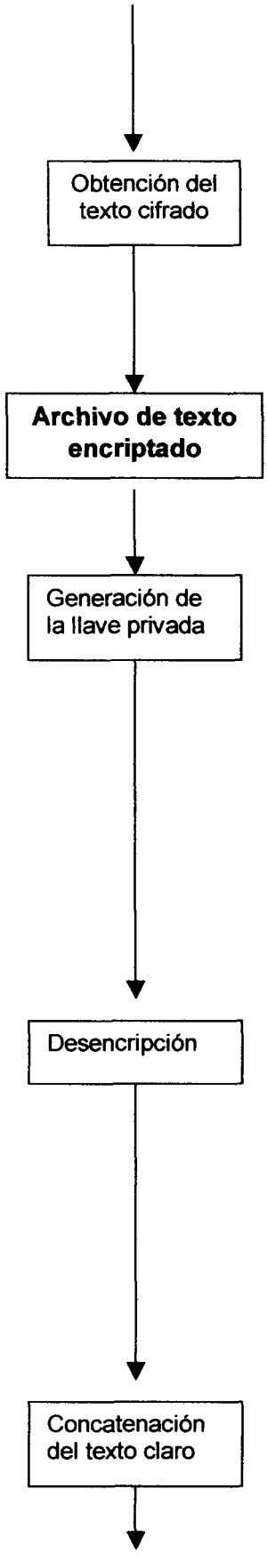


Figura 4.14 - Estructura básica del algoritmo de llave pública

El algoritmo básico que se encarga de una encripción del tipo RSA tiene varios inconvenientes para que sea aplicado de una manera sencilla, ya que su utilización en su forma más básica requiere de conocer mas acerca del funcionamiento del MAPLE, realizar correctamente las operaciones, saber donde colocar el texto en claro y en que parte y como se guarda el texto encriptado. Por ello se hizo la interfase más amigable para una mejor experiencia al utilizarla, además se le agregaron algunas líneas de código para que se pueda reconocer un gran número de caracteres y que el algoritmo no se limite a la encripción de letras. Con los

cambios agregados a la estructura básica, ahora se tienen dos archivos, uno para la encripción y otro que se encarga de la desencripción, además de que tanto el mensaje como los números que son las bases para dos llaves públicas y la llave privada se introducen por medio de archivos de texto que se pueden escribir cómodamente desde cualquier editor de texto para computadora. Para poder comprender mejor lo expuesto, se muestra en la figura 4.15 un diagrama a bloques, agregando las líneas de código que fueron necesarias para el mejor funcionamiento de la interfase del algoritmo.





En este bloque se utilizan las llaves públicas para la encripción de los números y agregan líneas para que se haga una conversión a números binarios y posteriormente que se genere un archivo con todos estos valores binarios.

```
Sección del algoritmo donde se encriptan
con las llaves públicas los valores en
las variables

for x1 from 1 to size by n1
do
code2(x1):=convert(code(x1),binary):
od:
 save
size,n1,p1,code2,"C:\\WINDOWS\\Escritorio\\RSAcrip
file";
```

Este es un nuevo bloque que se tiene que agregar para la obtención de la llave privada a partir del archivo de llaves públicas "publics.txt" y del archivo encriptado "RSAcripfile"

```
read "C:\\WINDOWS\\Escritorio\\RSAcripfile":
read "publics.txt":.....
Sección del algoritmo donde se genera la
llave privada a partir de las llaves
públicas
```

En este bloque se aplican las operaciones para la desencripción por medio de la llave privada. Aquí se agregan líneas para que el algoritmo haga primero una conversión de binario a decimal y posteriormente pueda desencriptar todos los tipos de caracteres que se le agregaron.

```
for x1 from 1 to size by n1
do
code(x1):=convert(code2(x1),decimal,binary):
od:

Sección del algoritmo donde se hace la
desencripción por medio de la llave
privada
> elif ad(x1)=27 then bd(x1):="A";...
> elif ad(x1)=52 then bd(x1):="Z";...
> elif ad(x1)=53 then bd(x1):="0";...
> elif ad(x1)=62 then bd(x1):="9";...
> elif ad(x1)=64 then bd(x1):=",";...
> elif ad(x1)=80 then bd(x1):=")";...etc
```

En este bloque se concatenan los caracteres para volver a formar un mensaje coherente. Se agregan las líneas que permiten se forme un nuevo archivo de texto simple de nombre "RSAtexclar2.txt".

```
Sección del algoritmo donde se concatenan
los caracteres para volver a formar el
mensaje.
save
mensaje2,"C:\\WINDOWS\\Escritorio\\RSAtexclar2.txt";
```

Archivo de texto desencriptado

Figura 4.15 - Estructura del algoritmo de llave pública utilizado

En la figura 4.16 se aprecia el diagrama en bloques del proceso completo del algoritmo de llave pública.

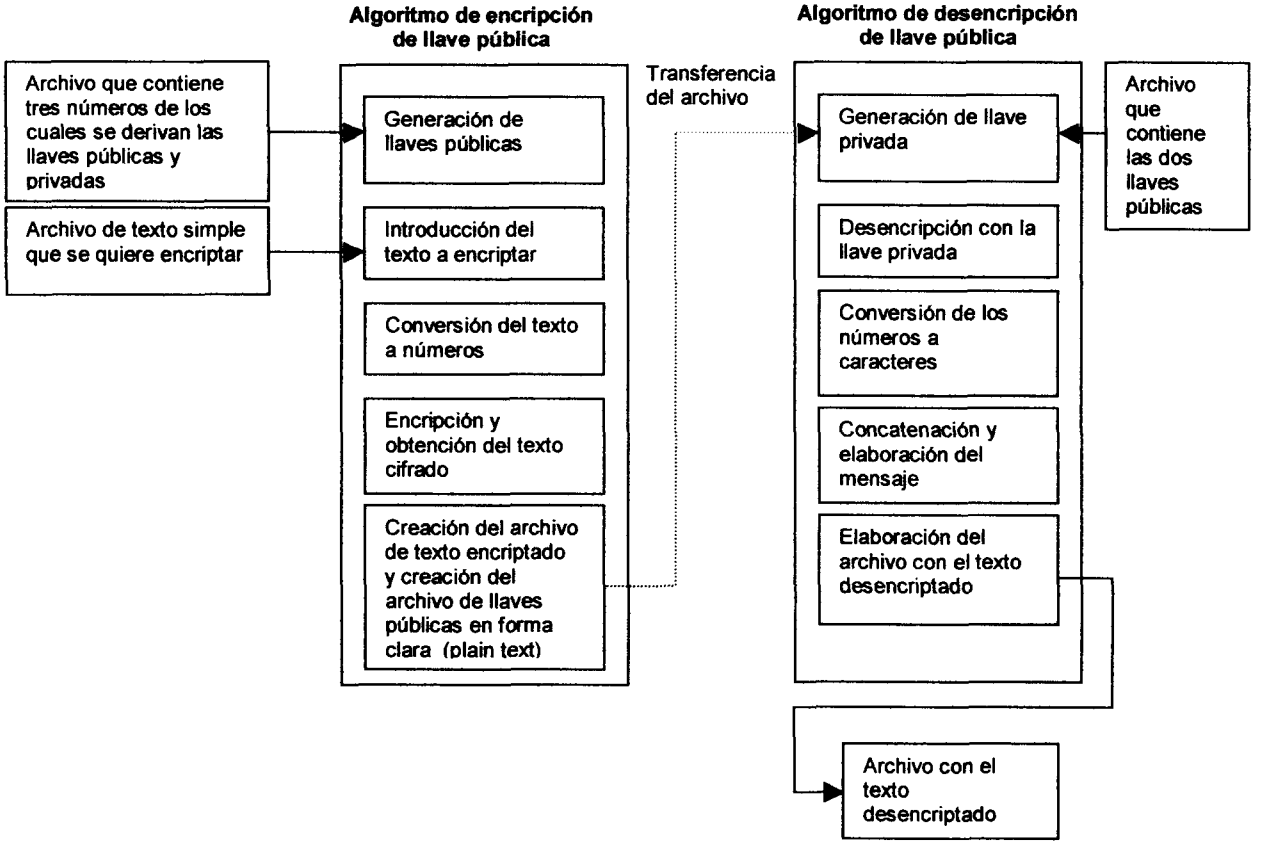


Figura 4.16 - Algoritmo de llave pública

Las pruebas con este algoritmo de llave pública se hicieron con párrafos de texto, ya que la mayoría de los mensajes que se desean encriptar están en este formato. Para tener un buen punto de comparación del funcionamiento de este algoritmo, se implemento un algoritmo de llave privada en MAPLE, y su explicación se presenta enseguida.

Estructura del algoritmo de llave privada

El algoritmo de llave privada implementado en MAPLE esta basado en el DES (Data Encryption Standard). El precursor del algoritmo DES fue el ***Lucifer*** un algoritmo desarrollado por IBM. Lucifer era largo, pero candidato directo para su implementación iterativa en un programa de computadora. Además, a diferencia de los algoritmos Merkle-Hellman y RSA, que usan aritmética sobre números binarios de 100 o 200 dígitos, Lucifer usaba solo operaciones lógicas simples en cantidades relativamente pequeñas. Posteriormente, un algoritmo de encripción de datos basado

en Lucifer fue desarrollado por IBM, este algoritmo se volvió conocido como DES, aunque su nombre correcto es DEA (Data Encryption Algorithm) en los Estados Unidos y DEA1 (Data Encryption Algorithm-1) en otros países.

DES fue adoptado como estándar federal 23 de los Estados Unidos en Noviembre de 1976. Su uso fue autorizado para aplicación en los sectores públicos y privados de comunicación no clasificada. Mas tarde seria aceptado como un estándar internacional por la Organización Internacional de Estándares. El algoritmo DES se basa en la aplicación de sustituciones, permutaciones, corrimientos de bits y aplicación de OR exclusivo a un mensaje dividido en bloques de 64 bits en conjunto con la llave privada, que debe ser también de 64 bits, aunque inmediatamente a su aplicación se reduce a 56 bits. Para descifrar el mensaje se necesita conocer la llave privada, la cual solo deben saberla quien envía el mensaje y el destinatario.

En la figura 4.17 se muestra la estructura básica en bloques del algoritmo de encripción de llave privada implementado en MAPLE:

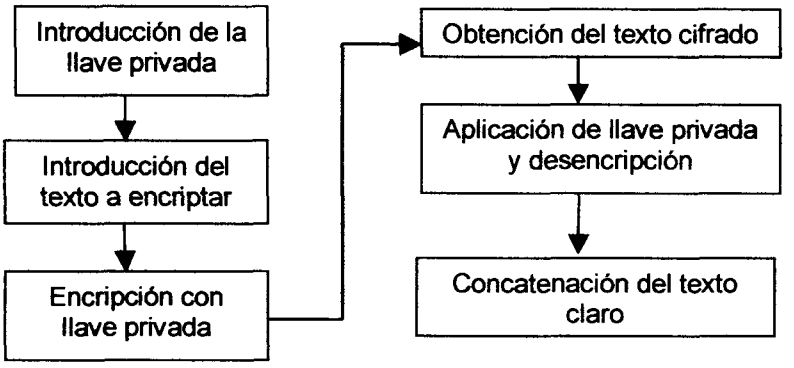
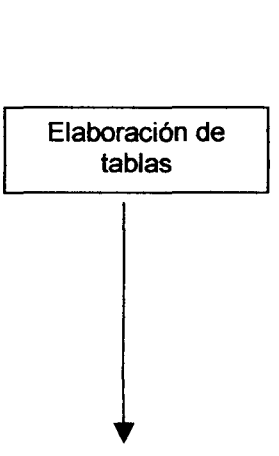


Figura 4.17 - Estructura básica del algoritmo de llave privada

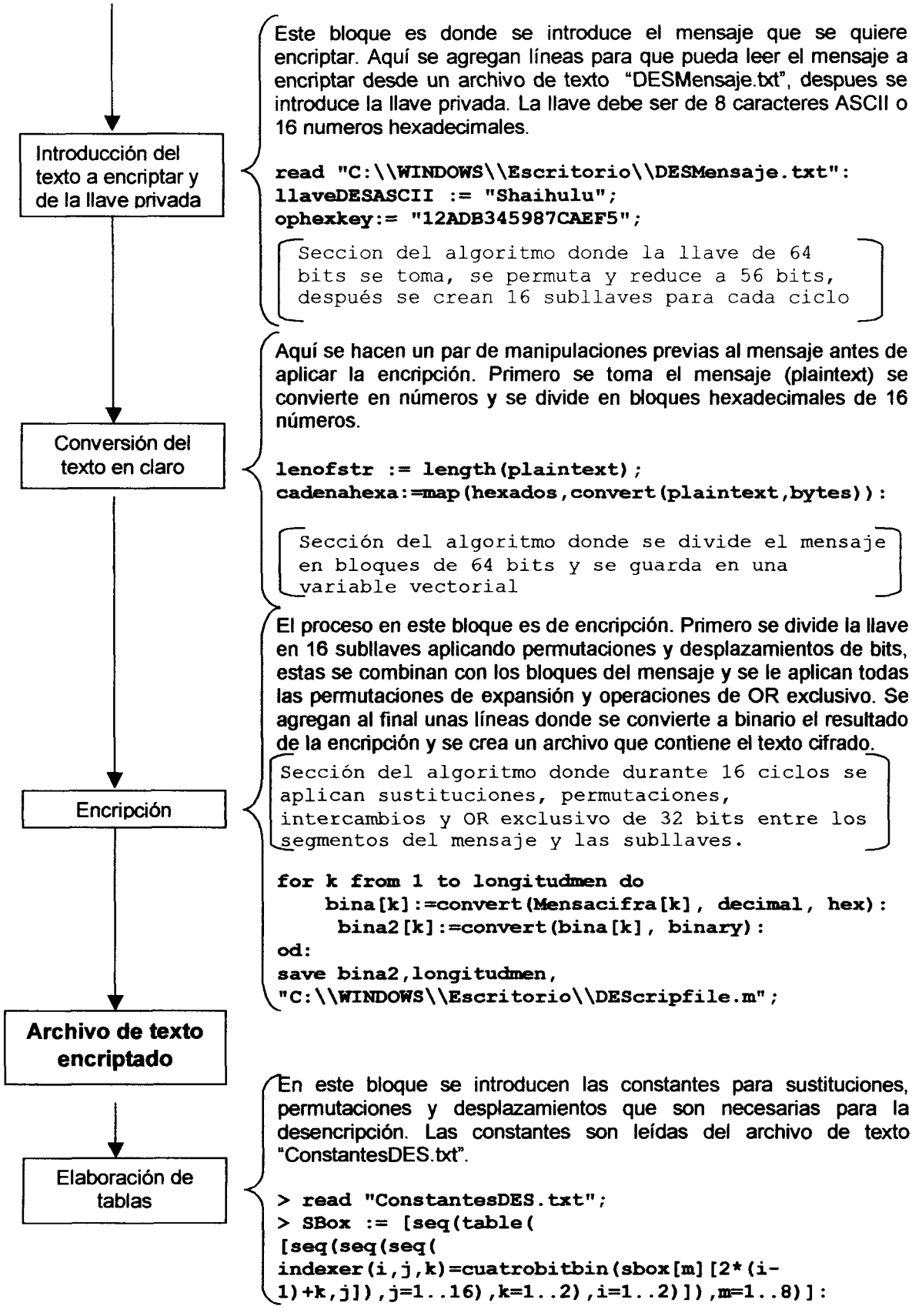
Una encripción aplicada en MAPLE del tipo DES tiene varios inconvenientes si se busca utilizar directamente, requiriendo de mayor conocimiento de MAPLE para introducir el texto a encriptar y las tablas de constantes necesarias para la encripción. Es por ello que se hicieron ajustes en su interfase para poder tener una mejor experiencia al hacer uso de la encripción de mensajes. Se agregaron líneas de código para introducir las tablas de sustitución y permutación. Otro de los cambios es que ahora se tienen dos archivos de código MAPLE, uno para la encripción y otro para la desencripción de mensajes. El mensaje a encriptar llega al programa en MAPLE desde un archivo de texto simple que se pueden escribir cómodamente con cualquier editor de texto su sencilla utilización, con la intención de hacer más fácil.

En la figura 4.18 se muestra el diagrama a bloques, agregando las líneas de código necesaria para un mejor funcionamiento de la interfase del algoritmo.



En este bloque se introducen las constantes para sustituciones, permutaciones y desplazamientos que hace mas adelante el algoritmo. Las constantes son leidas del archivo de texto "ConstantesDES.txt". Y se convierten las matrices de constantes en las tablas Sbox.

```
> read "ConstantesDES.txt";
> SBox := [seq(table(
[seq(seq(seq(
indexer(i,j,k)=cuatrobitbin(sbox[m][2*(i-
1)+k,j]),j=1..16),k=1..2),i=1..2)]),m=1..8)]:
```


Introducción del texto a encriptar y de la llave privada
Este bloque es donde se introduce el mensaje que se quiere encriptar. Aquí se agregan líneas para que pueda leer el mensaje a encriptar desde un archivo de texto "DESMensaje.txt", despues se introduce la llave privada. La llave debe ser de 8 caracteres ASCII o 16 numeros hexadecimales.
read "C:\\WINDOWS\\Escritorio\\DESMensaje.txt":
llaveDESASCII := "Shaihulu";
ophexkey:= "12ADB345987CAEF5";
Seccion del algoritmo donde la llave de 64 bits se toma, se permuta y reduce a 56 bits, después se crean 16 subllaves para cada ciclo
Conversión del texto en claro
Aquí se hacen un par de manipulaciones previas al mensaje antes de aplicar la encripción. Primero se toma el mensaje (plaintext) se convierte en números y se divide en bloques hexadecimales de 16 números.
lenofstr := length(plaintext);
cadenahexa:=map(hexados,convert(plaintext,bytes)):
Sección del algoritmo donde se divide el mensaje en bloques de 64 bits y se guarda en una variable vectorial
Encripción
El proceso en este bloque es de encripción. Primero se divide la llave en 16 subllaves aplicando permutaciones y desplazamientos de bits, estas se combinan con los bloques del mensaje y se le aplican todas las permutaciones de expansión y operaciones de OR exclusivo. Se agregan al final unas líneas donde se convierte a binario el resultado de la encripción y se crea un archivo que contiene el texto cifrado.
Sección del algoritmo donde durante 16 ciclos se aplican sustituciones, permutaciones, intercambios y OR exclusivo de 32 bits entre los segmentos del mensaje y las subllaves.
for k from 1 to longitudmen do
bina[k]:=convert(Mensacifra[k], decimal, hex):
bina2[k]:=convert(bina[k], binary):
od:
save bina2,longitudmen,
"C:\\WINDOWS\\Escritorio\\DEScripfile.m";
Archivo de texto encriptado
Elaboración de tablas
En este bloque se introducen las constantes para sustituciones, permutaciones y desplazamientos que son necesarias para la desencripción. Las constantes son leídas del archivo de texto "ConstantesDES.txt".
> read "ConstantesDES.txt";
> SBox := [seq(table(
[seq(seq(seq(
indexer(i,j,k)=cuatrobitbin(sbox[m][2*(i-
1)+k,j]),j=1..16),k=1..2),i=1..2)]),m=1..8)]:

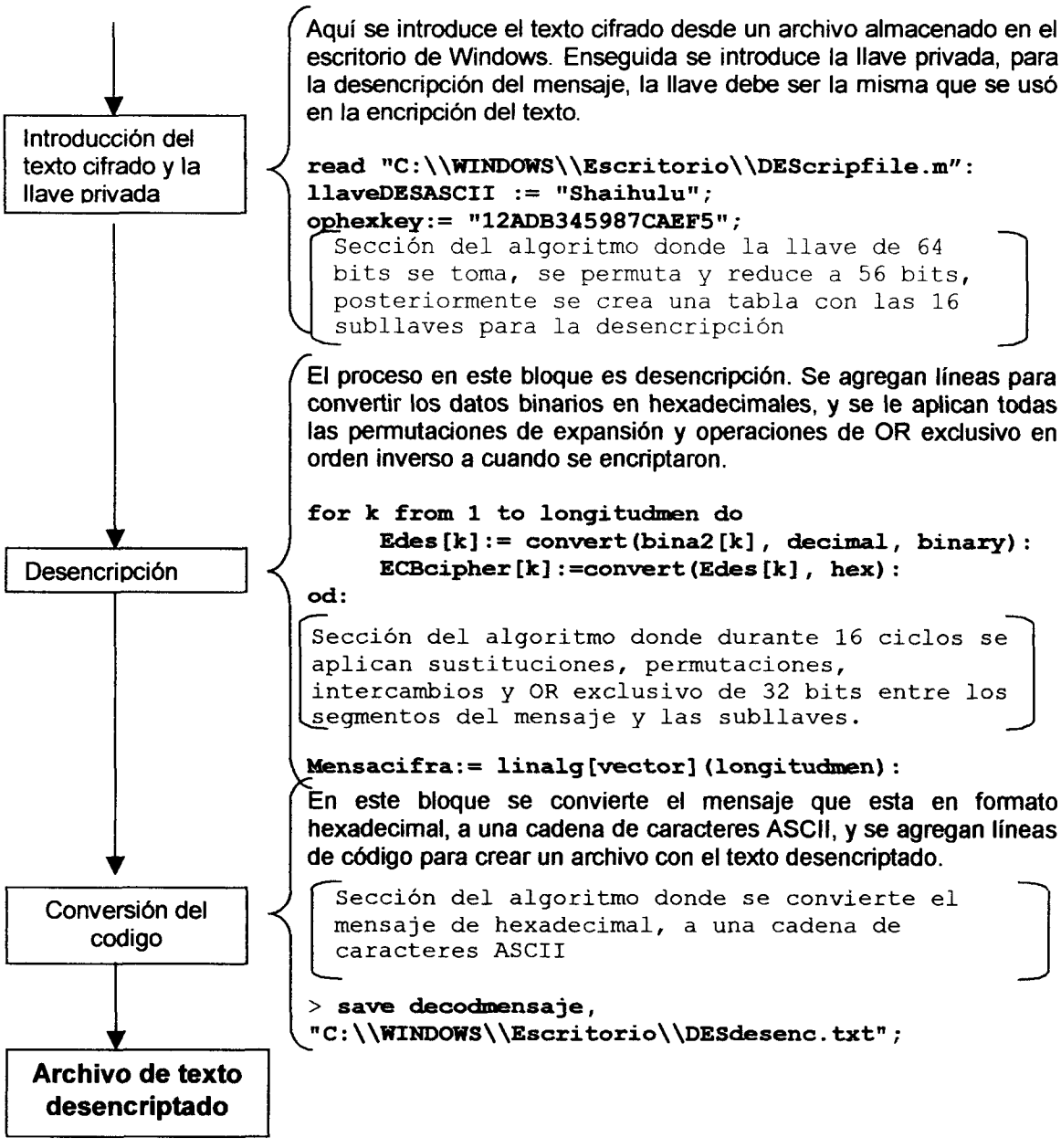


Figura 4.18 - Estructura del algoritmo de llave privada utilizado

En la figura 4.19 se define el proceso completo en bloques del algoritmo de llave privada.

Con este algoritmo de encripción por llave privada se hicierón pruebas con párrafos de texto y se compararón los resultados con los obtenidos de las pruebas de la encripción con llave pública, con la intención de apreciar mejor las ventajas y desventajas de cada sistema de encripción y obtener los datos suficientes para elegir de manera adecuada la opción que mejor se adapte a las necesidades de las comunicaciones del usuario.

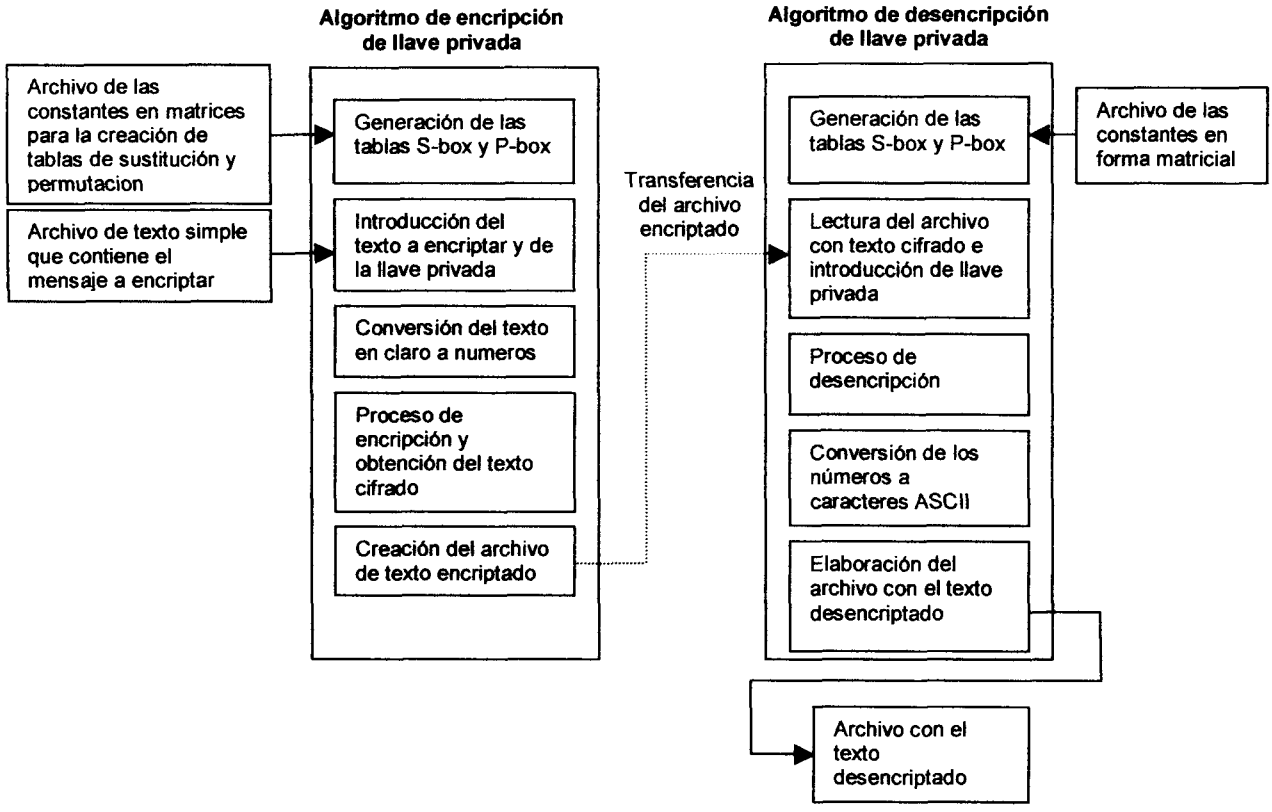


Figura 4.19 - Algoritmo de llave privada

Equipo y Características de Red Para Pruebas

Las pruebas que se realizaran con los algoritmos y los archivos encriptados con los programas encontrados en Internet consistirán en observar el tiempo de procesamiento, tamaño de los archivos antes y después de la encripción, y en el tiempo de transferencia entre computadoras.

Para el monitoreo de las transferencias se utilizó una red compuesta de dos computadoras manejando el sistema Windows XP y Windows Millenium.

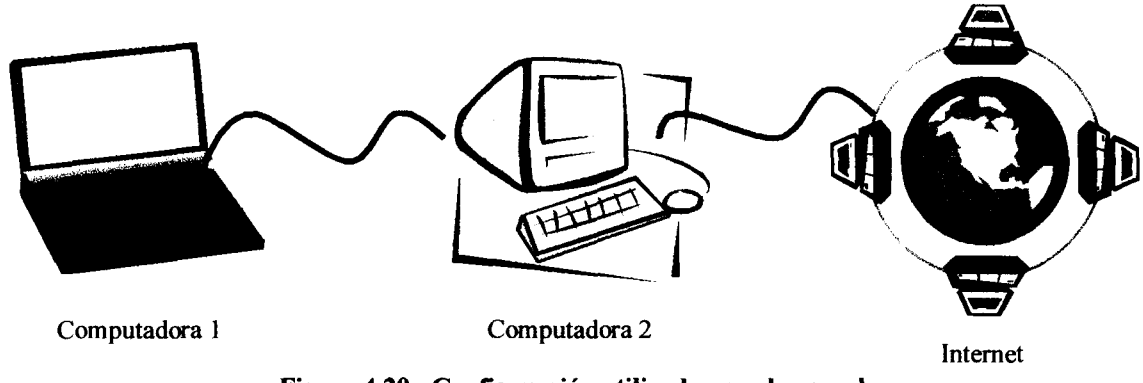


Figura 4.20 - Configuración utilizada para las pruebas

Tabla 4.7 - Características de las computadoras

Características	Computadora 1	Computadora 2
Sistema operativo	Windows Millenium	Windows XP
Disco duro	6 Gb	40 Gb
Procesador	Intel Celeron	Intel Pentium IV
Velocidad	766 Mhz	1.8 GHz
Memoria RAM	64 Mbytes	256 Mbytes
Conexión	Conexión a Internet del tipo Ethernet a la Computadora 2	Conexión a Internet por modem
Dirección de IP	192.168.0.233	192.168.0.1

En la figura 4.21 se puede ver el programa de monitoreo (*sniffer*) utilizado: **NetworkActive Sniffer v1.4.2.2**.

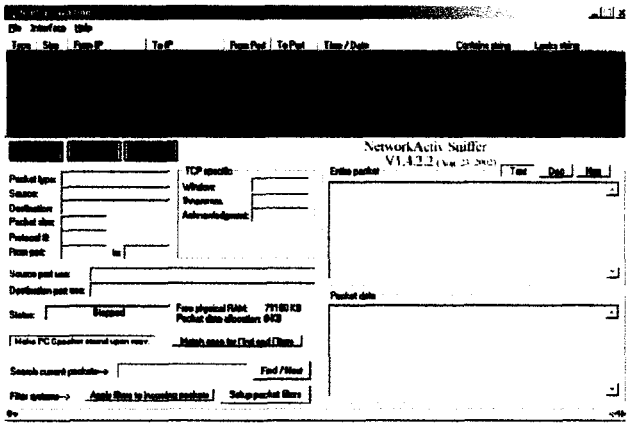


Figura 4.21 - NetworkActive Sniffer v1.4.2.2

Los otros programas utilizados para la encripción de la información fueron:

- **Crypto v3.9 Copyright 1986-2002 by Gregory Braun,** quien utiliza un algoritmo Blowfish de llave simétrica para la encripción de los archivos.

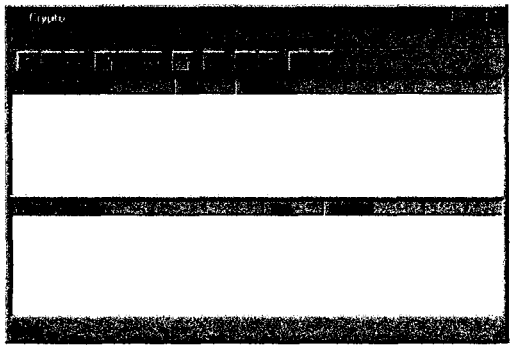


Figura 4.22 - Crypto v3.9

- **Advanced Encryption Package 2003 v1.8.1,** Este software nos presenta distintas alternativas en cuanto al uso de algoritmos de encripción. Cabe destacar que todos son del

tipo de algoritmos de encripción simétrica, es decir que con una sola llave encriptan y desencriptan. Entre los algoritmos que nos permite usar este programa están:

Tabla 4.8.- Algoritmos soportados por el AEP

Algoritmo	Tamaño de la llave
Blowfish	448 bits
Rjndael	256 bits
CAST	256 bits
Triple DES	192 bits
RC2	1024 bits
Diamond 2	2048 bits
Tea	128 bits
Safer	128 bits
3-Way	96 bits
Gost	256 bits
Shark	128 bits
Square	128 bits
Skipjack	80 bits
Twofish	256 bits
Mars	448 bits
Serpent	256 bits

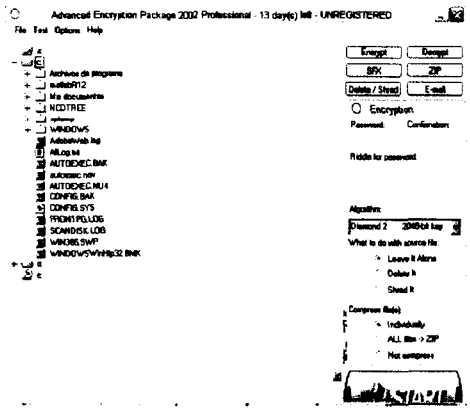


Figura 4.23 - Advanced Encryption Package 2003 v1.8.1

- **CS Enigma v1.4.0000,** También nos ofrece distintos tipos de algoritmos de llave simétrica para la encripción de los datos y archivos, los podemos ver en la tabla 4.9:

Tabla 4.9 - Algoritmos soportados por el CS Enigma

Algoritmo	Tamaño de la llave
DES I	8 bytes
Rjndael	32 bytes
Blowfish	56 bytes
Triple DES	24 bytes
CAST-128	16 bytes
Safer +	32 bytes
Twofish	32 bytes
Mars	32 bytes
Serpent	32 bytes

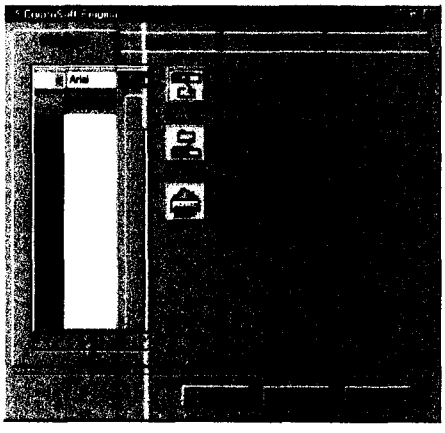


Figura 4.24 - Enigma v1.4.0000

- **CES Encryption Utility, Versión 1.12 Build 0004.** Este software no utiliza ningún algoritmo conocido públicamente sino que más bien es un algoritmo propietario simplemente llamado CES de encripción de llave simétrica.

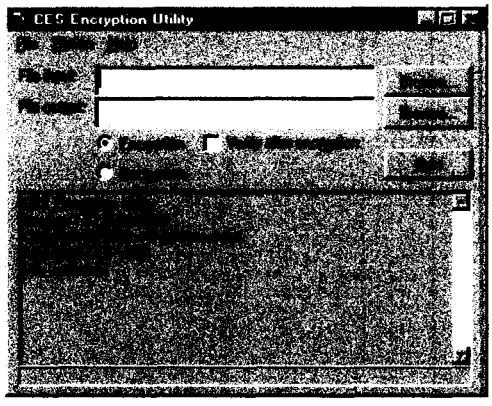


Figura 4.25 - CES Encryption Utility, Versión 1.12 Build 0004

Estos se utilizaron porque son programas comunes que se pueden encontrar en Internet y pueden probarse durante cierto tiempo o bien son programas libres de cargo. Estos programas proveen solamente de algoritmos de llave privada ya que son los más fáciles de utilizar por un solo usuario para la seguridad de sus archivos. Ciertamente no son programas que presenten las características de los algoritmos de llave pública y privada utilizados en MAPLE, sin embargo se probaran estos programas como punto de comparación para ver el tiempo que toma la encripción de los archivos de llave privada y además de poder ver que tanto aumenta de tamaño y el tiempo que toman la transmisión de estos archivos de una computadora a otra. Los programas de encripción pueden usar tres de ellos el algoritmo Blowfish, se utilizara este para ver los resultados y así saber las diferencias entre estos y posteriormente ver el comportamiento del algoritmo de llave pública basado en RSA y del algoritmo de llave privada basado en DES. Los archivos que se encriptarán con llave privada serán exactamente los mismos para probar como se comportan los distintos programas de criptografía. Así podremos saber la exigencia que tiene del hardware o de la red y hacer una comparación con los programas más comerciales. Por la misma razón los mensajes encriptados con el algoritmo de llave pública implementados en MAPLE serán exactamente los mismos que los encriptados con el algoritmo de llave privada en MAPLE.

Para probar el uso de los programas de encripción que se descargaron, se encriptarón algunos archivos de texto y en los cuales se midió el tamaño original y el tamaño después de la encripción, al mismo tiempo que se cuenta el tiempo que se tomo para la codificación. En las tablas 4.10, 4.11, 4.12 y 4.13 se muestran los resultados obtenidos.

Tabla 4.10 - Resultados con CS

Formato	*Tamaño del archivo*	*Tiempo de encripción*	*Tamaño después de encriptar*	*% de diferencia de tamaño*
Texto	**7.13k**	**<1 segundo**	**319k**	**+4374%**
Texto	**13.1k**	**00:00:01**	**321k**	**+2350%**
Texto	**167k**	**00:00:01**	**362k**	**+116.7%**

Tabla 4.11 - Resultados con Advanced Encryption Package

Formato	*Tamaño del archivo*	*Tiempo de encripción*	*Tamaño después de encriptar*	*% de diferencia de tamaño*
Texto	**7.13k**	**<1 segundo**	**3.95k**	**- 44.6%**
Texto	**13.1k**	**1.5 segundo**	**6.62k**	**- 7.15%**
Texto	**167k**	**1.8 segundo**	**63.3k**	**- 62 %**

Tabla 4.12 - Resultados con Crypto v3.9

Formato	*Tamaño del archivo*	*Tiempo de encripción*	*Tamaño después de encriptar*	*% de diferencia de tamaño*
Texto	**7.13k**	**<1 segundo**	**7.40k**	**+ 3.78%**
Texto	**13.1k**	**<1 segundo**	**13.3k**	**+ 1.52%**
Texto	**167k**	**<1 segundo**	**168k**	**+ 0.59%**

Tabla 4.13 - Resultados con CES Encryption Utility

Formato	*Tamaño del archivo*	*Tiempo de encripción*	*Tamaño después de encriptar*	*% de diferencia de tamaño*
Texto	**7.13k**	**0:00:00.100**	**8.13k**	**+ 14.02%**
Texto	**13.1k**	**0:00:00.241**	**14.1k**	**+ 7.63%**
Texto	**167k**	**0:00:02.688**	**168k**	**+ 0.59%**

En la figura 4.15 la estructura a bloques especifica que el algoritmo de llave pública basado en RSA genera un archivo que contiene el vector con los datos producto de la encripción y previo a la creación de este archivo, el vector es convertido a números binarios. Para mostrar su operación y resultado se encriptará el siguiente párrafo de texto:

"Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as work in progress."

Este texto se introduce al programa de encripción en un archivo ***.txt***, los números con los que se generan las llaves se introducen por medio de otro archivo ***.txt***. Para este ejemplo los números son: 800908867, 6699876556, 2987678933724245001. Estos números se encargan de generar llaves públicas de 64 bits y la llave privada del receptor también será de 64 bits. Al efectuarse la encripción se obtiene un vector con datos cifrados en forma binaria, este se guarda en un archivo que se envía al destinatario. Para este ejemplo el archivo contiene lo siguiente:

code2(181):=10101100110101010110110100001110111011010110001010100100010111;code2(241) :=10101011111010101000111001000010101111111011010000001001 1;code2(61) :=11111000100100011011000101001001111001111100111110010101 01;code2(121) :=10101101000001111001101010001100100 0

11110000100011010010011 01;code2(1) :=1100010001111111001100001000110110100110110011101000001101101111;code2(246):=1000011101011111000001100011010100101010110100011010110111100 11;code2(126):=1111010100000111111001001111000110010111000010000001111101000 1;code2(186):=1100001010100000011101111111010011110101000101000000000011010;code2(6):=1010001100011001010011101111011010111010000011000110011011010111;code2(66):=1010111100011111101111110011010101100001001100011101110001 0;code2(191):=1011000100101011100111100011011001001100100001100110101010110 1;code2(251):=1010111110100011001001011000110101110110000000111000100000100;code2(71):=1001001110000001000101110110001101111101101100001000011110000 01;code2(131):=1001101010001001111101001110011110100100101100010101101110001 0;code2(11):=1101110101101110001100111000011101010000 10;code2(196):=1000000011111001111101111010101111100111000010100011110000110101000 10;code2(256):=1011001110000100000111101000001011110010001110011011101101110101101000001;code2(76):=1101011111111001011100100000001100111110101110100101100000000;code2(136):=1100010000010110101011010101000111010001101000000011001110010;code2(16):=1000010010100010000101111000001110100011011111000000011110010 10;code2(141):=1111011001100001000010100110110001000000100110011101011001000 0;code2(201):=1001110011000011001011111001100110010100001000100110011101011 0;code2(21):=1110100100100000000101110100100000110111101001001111000011000;code2(81):=1010000000001111100001101111001000011000001100100100101010 0;code2(206):=1100111001001111111001100101011101010000110010010010110101000;code2(86):=1111011011001100010001001111101000111001100000110;code2(146):=1101010011000101101001000101010110010000100001100100011011101 0;code2(26):=1010011101000110011011101000001111000111111111111110;code2(151):=1000001101111111011011000111101101011011111110001000001001010001;code2(211):=1110000100100101110001111000011001111010010101111111101010001;code2(31):=1000100100011000100011110100011010100110101001111111011111011111;code2(91):=1110110010101100100110100000001111110001110011101001001000 0;code2(156):=1110000111100011101110111110100010101101010001110101011101011 0;code2(216):=1111011111111101000010010101101000010111010011111101001100;code2(36):=1000110010000101010000100110100000100000011000111010101001111;code2(96):=1010010010000110101011011011101111010010111110100011010111010;code2(221):=1100111100000011110011100101011001110010000100111000011011000 0;code2(101):=1100000110011001100000010110011000110010110111101101011110001;code2(161):=1000010010101011110101100111000100110011010001110010111101010;code2(41):=1100011110111110100000000011100111011100001100110100111010 1;code2(166):=1010011111010100000110010010100000000011111111110110101110011;code2(226):=1100011001111110110101011101010011111011001010011001011000101;code2(46):=1100111001010100010000010001101110101110001110011111110111001;code2(106):=1110010111011010000010011010000000001100101101010111101010100;code2(231):=1010100100010011000000011011011000010001001010010001010011000;code2(111):=1000101010111011000111011011111001101010011001101011100010000;code2(171):=1010101110101101100111110000010110101110111111110110011;code2(51):=1110100111011111110110111101111110001110101100000110011000101 00; code2(236) :=1000111011110001000110001110010101011110100111100101010000 001; code2(116) :=1100011001111110110101011101010011111011001010011001011000101;code2(176):=1111111010011111101011000011101001001110011111011000100111101;code2(56):=1111010101100110100111000011100010000110110000010010000101010;

En la figura 4.18 se muestra la estructura del algoritmo de encripción por llave privada basado en DES, ahí se especifica que el texto es convertido en números y, al igual que en el algoritmo de encripción por llave pública, se genera un archivo que contiene un vector con los datos producto de la encripción, los datos en el vector están en formato binario. Este es el archivo que se envía al destinatario, quien debe desencriptarlo. Para mostrar el resultado de una encripción con el algoritmo de llave privada se encripta el mismo párrafo de texto utilizado como ejemplo para el algoritmo de llave pública. Con este algoritmo se utiliza una llave privada de 64 bits o de 8 caracteres ASCII.

"Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as work in progress."

El archivo que se genera contiene la siguiente información:

bina2:=table([(1)=10111101101111000111010111100011001110111010011110010100111100,(2)=110101
01100010111110111100010010010010000000001101111101001111,(3)=11011111100011010111001110
01100100101001000001110100111,(4)=11111100101011101011011101100111011100110011111111000
00101,(5)=10000110001101001011101010110111001001010100000111110010010110 10,(6)=1001001110
11000111010000011001000101011101001101111111101111101 01,(7)=11001010101101101100111111100
11110100101110100111101101111011101,(8)=10001100101101100101010110111111011011011000101
010011100001000,(9)=11111111100110110000011000010101100100010100011100110011011111001,(10)
=10011010001011100011101111000111111000100000001011001111010111 1,(11)=101101111010111111
01111000010101001111110011001110100111000111 00,(12)=11100110100101111000111111001010111 0
11100110001011110001101111 00,(13)=10101001001110101101010000100101010011111100011001110111
1001110110,(14)=11100111110011011000000101010100000000011110001000101011110 11,(15)=1101100
10110111111010101101110100111100111001110101100011010001 0,(16)=11011011001110101010100 11
11110101011011000101001011000000001101101,(17)=10001000111100001001101101111111110011100 00
11010100100100101011,(18)=11111101010110001010001101100001110010100010011011011001101111
01,(19)=11100010101101111011100100111001111101001101010101011011110011 10,(20)=11100010110
11110011101011001011110101111101011000010010000 10010,(21)=11110101110100000000100110000 0
00111110010011001010111111100100100,(22)=10100000011100011000001011100110001011000110001 1
0010111110110101,(23)=10010011010111001001011110100101001101001101111001110101110000 00,(2
4)=10000110000000000010010010101011100010000101101101001110100011 10,(25)=1000111110100011
00010111111011001100101000000010000010000110110 1,(26)=10010111011010111000011100010000 11
00110001001011111101010010011 1,(27)=11111001111111101101100011100110110011111110011101100
0110010110,(28)=10110010111001110010010000000111110000101000100110110100000 11,(29)=100101
11000000001011010100101100001110001100110001111000001111,(30)=10011110101110010001111111
00100110111101100101011001100100000100,(31)=10101101100000000001101110011010001001101101 1
10010111011111101 1,(32)=10100011010000100010011001001001110101001010000111101101010010 00
,(33)=10111000100011011011101111110000010111111000111010100111111010010]);

Aplicando la encripción por llave pública y privada a párrafos de distinto número de palabras se obtienen los datos que se muestran en la tabla 4.14. Las pruebas de encripción se llevan a cabo en la computadora 1 de la figura 4.20. Para poder tener un mejor punto de comparación entre estas dos técnicas de encripción implementadas en MAPLE, se eligieron dos llaves públicas de 64 bits para el algoritmo basado en RSA, y una llave privada de 64 bits para el algoritmo basado en DES, además de que las palabras que se encriptan son exactamente las mismas para ambos métodos.

Tabla 4.14 - Tiempos de encripción del algoritmo de llave pública y del algoritmo de llave privada

Número de palabras	Tiempo de Procesamiento con algoritmo asimétrico	Tiempo de Procesamiento con algoritmo simétrico
1	2.8 seg	4.6 seg
2	2.9 seg	6.2 seg
3	3.4 seg	6.6 seg
4	3.7 seg	6.9 seg
5	5.1 seg	7.0 seg
6	6.7 seg	7.4 seg
7	9.1 seg	8.4 seg
8	11.8 seg	10.8 seg
9	14.9 seg	11.1 seg
10	17.7 seg	11.8 seg
20	68.6 seg	18.0 seg
30	304.2 seg	24.5 seg
40	414.7 seg	29.5 seg
50	505.0 seg	36.4 seg
60	626.0 seg	43.1 seg

Si se observa los resultados en las tablas y al hacer una comparación del funcionamiento del algoritmo de llave pública y del algoritmo de llave privada, se puede ver que la exigencia en recursos del sistema y en poder de procesamiento del algoritmo de llave pública es mayor a la mostrada por el algoritmo de encripción de llave privada y los programas de encripción de Internet.

En la transferencia de archivos de la computadora 1 a la computadora 2 de la pequeña red mostrada en la figura 4.20, los archivos que se envían son previamente encriptados con los distintos programas de encripción por llave privada. También se envían los párrafos encriptados por los algoritmos de llave pública y de llave privada implementados en MAPLE. Con esto se quiere probar el peso de los archivos creados por medio de la encripción y así ver si su comportamiento es realmente aceptable para las operaciones que se sabe existen dentro de un ambiente de trabajo o de manera individual a cualquier usuario que quiera hacer transferencias seguras de archivos de datos.

Tabla 4.15 - Resultados con el CS Enigma

Formato	*Tamaño del archivo*	*Tamaño después de encriptar*	*% de diferencia de tamaño*	*Tiempo de transferencia*	*Número de paquetes transmitidos*
Texto	**7.13k**	**319k**	**+4374%**	**0.454 seg**	**234**
Texto	**13.1k**	**321k**	**+2350%**	**0.531 seg**	**236**
Texto	**167k**	**362k**	**+116.7%**	**0.625 seg**	**265**

Tabla 4.16 - Resultados con el Advanced Encryption Package

Formato	*Tamaño del archivo*	*Tamaño después de encriptar*	*% de diferencia de tamaño*	*Tiempo de transferencia*	*Número de paquetes transmitidos*
Texto	**7.13k**	**3.95k**	**- 44.6%**	**0.188 seg**	**7**
Texto	**13.1k**	**6.62k**	**- 7.15%**	**0.203 seg**	**9**
Texto	**167k**	**63.3k**	**- 62 %**	**0.329 seg**	**49**

Tabla 4.17 - Resultados con Crypto v3.9

Formato	*Tamaño del archivo*	*Tamaño después de encriptar*	*% de diferencia de tamaño*	*Tiempo de transferencia*	*Número de paquetes transmitidos*
Texto	**7.13k**	**7.40k**	**+3.78%**	**0.203 seg**	**10**
Texto	**13.1k**	**13.3k**	**+1.52%**	**0.219 seg**	**14**
Texto	**167k**	**168k**	**+0.59%**	**0.469 seg**	**125**

Tabla 4.18 - Resultados con CES Encryption

Formato	*Tamaño del archivo*	*Tamaño después de encriptar*	*% de diferencia de tamaño*	*Tiempo de transferencia*	*Número de paquetes transmitidos*
Texto	**7.13k**	**8.13k**	**+14.02%**	**0.188 seg**	**10**
Texto	**13.1k**	**14.1k**	**+7.63%**	**0.219 seg**	**15**
Texto	**167k**	**168k**	**+0.59%**	**0.453 seg**	**125**

En las tablas 4.15, 4.16, 4.17 y 4.18 se definen el tamaño, el tiempo de transferencia y el número de paquetes en los que se dividió el archivo que se transfirió. Los archivos que se transmiten como ejemplos de encripción de los algoritmos de llave pública y llave privada contienen párrafos de 40, 50 y 60 palabras. Los resultados se pueden ver en las tablas 4.19 y 4.20.

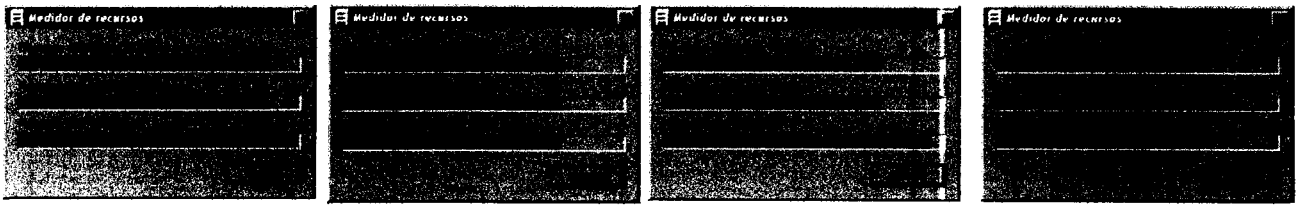
Tabla 4.19 - Datos obtenidos con el algoritmo de llave pública:

Archivo	Tamaño original del archivo	Tiempo de encripción	Tamaño después de encriptar	% de diferencia de tamaño	Tiempo de transferencia	Número de paquetes transmitidos
40 pal.	**240 bytes**	**414 seg**	**3869 bytes**	**+ 1512%**	**1.718 seg**	**11**
50 pal.	**306 bytes**	**505 seg**	**4889 bytes**	**+ 1497%**	**1.813 seg**	**12**
60 pal.	**373 bytes**	**626 seg**	**5996 bytes**	**+ 1507%**	**1.822 seg**	**14**

Tabla 4.20 - Datos obtenidos con el algoritmo de llave privada:

Archivo	Tamaño original del archivo	Tiempo de encripción	Tamaño después de encriptar	% de diferencia de tamaño	Tiempo de transferencia	Número de paquetes transmitidos
40 pal.	**240 bytes**	**29.5 seg**	**2145 bytes**	**+ 793%**	**1.698 seg**	**10**
50 pal.	**306 bytes**	**36.4 seg**	**2713 bytes**	**+ 786%**	**1.750 seg**	**10**
60 pal.	**373 bytes**	**43.1 seg**	**3354 bytes**	**+ 799%**	**1.765 seg**	**11**

En las tablas 4.19 y 4.20 se puede ver que para un archivo encriptado por llave pública es mayor el tiempo necesario de procesamiento, el texto encriptado es mayor que para uno encriptado por llave privada, el número de paquetes en que dividen los archivos es mayor para los encriptados por llave pública y el tiempo de transferencia es ligeramente mayor para los archivos encriptado por llave pública. Se puede apreciar que el algoritmo de llave privada proporciona una encripción a mayor velocidad y sus archivos encriptados ocupan un espacio pequeño. Otra de las mediciones que se efectuaron fue el uso de recursos del sistema de la encripción, se midió la utilización en la computadora 1 de la figura 4.20 y se utilizo el programa medidor de recursos del sistema Windows. En la figura 4.21a, se muestra que la utilización de recursos del sistema sin ningún programa y con el ambiente Windows corriendo fue de 14%, En 4.21b, se muestra que por medio del algoritmo de llave pública se utiliza un 24% y en 4.21c la encripción por llave privada es de 22%. Esto significa que cuando se encripta por llave pública se utiliza un 10% mas, y con la encripción privada es de un 8% mas de recursos de lo que el sistema usa normalmente. Esto significa que la encripción no es muy exigente en cuanto a recursos del sistema ya que en 4.21d, el programa Word de Microsoft Office utiliza un 28%, es decir un 14% mas de recursos.



a) b) c) d)

Figura 4.21 – Utilización de Recursos del Sistema

La robustez de los algoritmos ante la perdida de paquetes en una transferencia de archivos no es buena. Según se pudo observar en las pruebas de transferencias de archivos, algunos paquetes transportan en su *payload* aproximadamente el 30% del texto cifrado. La perdida de alguno de estos paquetes causaría que el mensaje no se pudiera recuperar, se necesita tener la totalidad de los paquetes que transportan el texto cifrado; en caso de que un paquete de los que llevan el texto encriptado se pierde, no quedaría suficiente información para realizar la desencripción; de hecho, la forma en que se encripta y desencripta la información exigen que no haya perdida de datos durante la transferencia de archivos. Cada bit contenido dentro de las variables que se envían en un archivo de texto cifrado es necesario para desencriptar la totalidad del documento. Esto es causado por la manera en que el proceso de desencripción se detiene si ocurre un error o faltan datos. Esta situación es valida para los métodos de encripción pública y privada implementados en MAPLE. En los archivos encriptados por métodos simétricos y asimétricos con que se hicieron las pruebas de transferencia, se observo que se necesitan entre 8 y 9 paquetes para definir el nombre y la ruta de grabación del archivo transferido, es decir que si el archivo fue dividido en 14 paquetes para su envío, 8 de esos 14 se encargan de la definición de rutas y nombre y 6 son los que llevan en su *payload* los datos que contiene el archivo. Si se trata de un archivo encriptado y se pierde uno de estos 6 paquetes con datos, la desencripción no se puede llevar a cabo. Dada esta situación seria necesario volver a transmitir el archivo hasta que se tenga el 100% de los paquetes.

Esto no debe ser un problema serio, porque generalmente los mismo protocolos de transferencia de archivos en una red local, se encargan de hacer automáticamente la retransmisión de un paquete que no llega a su destino. En las pruebas de transferencia con archivos encriptados se pudo observar que los sistemas se encargaban automáticamente de la retransmisión de los paquetes perdidos o dañados en su trayecto. Esto no fue común, ya que de 20 transferencias de archivos de alrededor de 3 Kbytes, solo en 2 ocasiones fue necesario retransmitir paquetes y aun con esta situación el tiempo de transferencia no se vio retardado ni en 1 milisegundo con respecto a cuando no hay perdidas de paquetes. Lo ideal es que no haya perdida de paquetes en una transferencia de archivos, pero eso sucede por el trafico, la prioridad y las políticas el sistema de la computadora, sin embargo esos temas no son el objetivo de esta Tesis.

Con los datos obtenidos en la encripción por llave pública implementada en MAPLE se puede observar que esta es demasiado tardada, requiriendo que el sistema se dedique exclusivamente a la encripción del mensaje y no se haga ninguna otra operación con el equipo. Así, de las tablas 4.19 y 4.20 los resultados en los tiempos son aproximadamente 13 veces más grandes en el algoritmo de llave pública implementado en MAPLE comparado con el tiempo de encripción del algoritmo de llave privada también implementado en MAPLE. Ciertamente que estos tiempos de encripción están derivados de la forma en que se hacen las operaciones en MAPLE, sin embargo, si se interpreta el mismo retardo para cualquier programa de encripción por llave pública estos serán demasiado lentos para cualquier aplicación computacional. Un administrador de red que quiera mandar mensajes confidenciales de 40 palabras a 20 usuarios y desee hacerlo por medio de la encripción por llave pública se tardara 138 minutos solo para encriptar todos los mensajes. Las actividades de un administrador a veces son holgadas pero si normalmente son demasiado exigentes como para perder tanto tiempo. Si se deseara hacer la encripción de los mensajes con algoritmos de llave privada el resultado sería de 9.8 minutos lo cual es mucho más razonable en cuanto a tiempo dedicado para una tarea. El tamaño de los archivos también es mucho mayor en la encripción por llave pública, siguiendo con el ejemplo de un administrador que deba enviar 20 mensajes encriptados a usuarios, con encripción de llave pública la cantidad de bytes a enviar sería de 77.38 Kbytes, no es una cantidad muy grande por si misma, y la transferencia de 20 mensajes tomaría alrededor de 34.36 segundos. Haciendo los mismos cálculos para la encripción por llave privada, tenemos que el total de datos a transferir es de 42.9 Kbytes y el tiempo de transporte es de 33 segundos. En el tiempo de transporte no hay mucha diferencia ya que si se compara individualmente un archivo encriptado por llave pública y un archivo encriptado

por llave privada, los tamaños son similares y es por ello que el tiempo en su conjunto es también similar. Al comparar los datos totales a transportar se observa que es menor en la encripción por llave privada en un 44.5%. Esto si se trata de un mensaje corto de 40 palabras, sin embargo con mensajes de 50 o 60 las diferencias serian aun mas marcadas. En si podemos afirmar que la encripción por llave pública no sería útil por el tiempo de encripción principalmente, los tamaños de los archivos generados y los tiempos de transferencia son parecidos para ambos métodos de encripción, pero la enorme cantidad de tiempo de la encripción asimétrica es algo que no se puede ignorar. Los sistemas DES y RSA son los más populares de cada método, y tienen varios años de estarse utilizando, casi todos sistemas que aparecieron después incluyen mas operaciones y llaves más largas por lo que los tiempos de encripción tienden a elevarse. Si la encripción se quiere aplicar por software, el proceso seria muy tardado, se puede decir que a partir de que un sistema tarde 10 segundos en encriptar un mensaje este ya es lento, por ello muchas compañías dedicadas a la seguridad diseñan dispositivos periféricos a la computadora que ese encargan de la transmisión encriptada de los archivos o paquetes de datos. Sin embargo, para propósitos de comparación, estudio, pruebas y análisis la encripción por software es la mas útil y realizable, además de que el comportamiento a escala es similar. Es decir, un dispositivo dedicado a la encripción por llave pública se tardará mucho más en la encripción que uno de llave privada.

Con los resultados obtenidos de estas mediciones en la transferencia de archivos encriptados y poniendo atención en el tiempo de procesamiento de la encripción se puede ver que la encripción por llave pública es un proceso más largo pero su algoritmo permite que esta sea más segura que la encripción por llave privada. La encripción por llave privada es más rápida y esto se puede ver en la encripción en MAPLE y en la encripción con los programas de llave privada descargados en Internet, aunque esto depende del programa de encripción que se utilice, ya que algunos pueden aumentar mucho el tamaño de los archivos. Sin embargo la seguridad de los programas de encripción por llave privada no es muy alta, ya que depende de una sola llave. Los algoritmos de llave pública serían mas apropiados para utilizarse cuando se trate de párrafos no muy grandes de texto, como para transmitir llaves, o en la elaboración de firmas digitales para un documento, así el tiempo gastado en la encripción será poco. Para el caso en que se necesita transferir un archivo grande y encriptarlo con llave pública, lo recomendable sería dividirlo en varios archivos de párrafos pequeños y así no resentir tanto el tiempo que consume la encripción, al hacer esto se puede cambiar la llave para cada sub-archivo asegurando aun más la privacidad de este documento.

Con las recomendaciones hechas al inicio del capitulo para proteger distintas configuraciones de sistemas de computo y los resultados obtenidos en cuanto al procesamiento y transferencia de archivos encriptados se pueden tener una idea de cuales son las mejores decisiones a tomar cuando se quiera tener un sistema seguro y una transferencia igualmente segura.

CONCLUSIONES

La seguridad en Internet siempre ha sido una de las principales preocupaciones para todos aquellos que están conscientes de los peligros que puede ocasionar una intrusión de alguien no deseado en nuestra propia computadora o en los archivos más secretos. Como hemos visto no solo debemos de cuidarnos de aquellos quienes están fuera de nuestra casa u oficina sino también de quienes son compañeros de trabajo. La información es una posesión muy valiosa, no debemos de dejar que alguien husmee sin consentimiento.

Hemos visto las definiciones y como se encuentra la situación hoy en día, así como las principales organizaciones que están trabajando en estos problemas. Esta no es un acción fácil ya que siempre habrá gente que tome como reto el acceder de manera ilegal a cualquier sistema o archivo que esta conectado a Internet. Muchas de estas personas tienen la firme creencia de que están haciendo algo bueno al mostrar las fallas en los sistemas de seguridad, ya que ellos no hacen ningún daño a los archivos personales. Sin embargo hay quienes no tienen buenas intenciones y se la pasan explorando las posibilidades de observar o modificar información ajena. Se podría decir que esta es una característica típica del hombre ya que siempre le gusta tomar lo que esta prohibido y aun en el ambiente electrónico esto se aplica porque siempre se están buscando maneras de romper las modernas protecciones a la información.

Los clásicos sistemas de seguridad como la encripción, antivirus y *firewalls* son los mas útiles para tener una buena privacidad en la transferencia de los datos, sin embargo no son perfectos, los piratas siempre encuentran puertas traseras y formas de entrar. Los algoritmos y las funciones *hash* se hacen más complejos con el paso del tiempo ya que cada vez es más difícil para mantener intacta y sin conocer los datos que estamos transportando. Aun existe mucha investigación para mantener la información segura, algunos trabajos se orientan en que se puedan hacer cada vez mas modificaciones a los algoritmos de encripción y a las funciones *Hash* para que resistan los ataques más usuales, evitando así, que haya incursiones y protegiéndonos de robos de archivos. El diseño de nuevos protocolos es algo complicado por todos los recursos que se necesitan para esto, aunque también para la modificación de los algoritmos sin embargo el protocolo incluye muchas mas cosas y un algoritmo es básicamente un programa que interactúa con el hardware.

Con la realización de este proyecto se logró definir los algoritmos de encripción más comunes, una comparación y como es el funcionamiento de ellos, así como de las funciones *Hash*. Al mismo tiempo se presento una visión sobre los protocolos de seguridad en Internet y los niveles o capas en que trabajan ellos. Se expuso el funcionamiento de la seguridad en Internet a partir de la aplicación del protocolo IPv6 con sus nuevas características, y se mencionaron todos los elementos que conforman la seguridad computacional, incluyendo las principales amenazas, casos de ataques conocidos y recomendaciones informáticas dedicadas a mantener un sistema seguro.

En el capitulo 4 se analizaron distintos tipos de circunstancias que se presentan al tratar de definir diversos sistemas de computación que pueden tener vulnerabilidades, se agregaron los consejos necesarios aunque dejando un tanto de libertad para los distintos usos o necesidades de privacidad que se deseen tener. Se consideran diversas recomendaciones para estas configuraciones, quizá no sean todas las que existan pero son las más comunes y en ciertos casos las más fáciles de implementar. Uno de los puntos más importantes dentro de esta investigación fue el poder realizar pruebas con los algoritmos de criptografía implementados en MAPLE de llave pública y de llave privada, comprobamos que funcionan de manera correcta con cantidades no muy pesadas de texto y su estabilidad es buena, aunque que para grandes cantidades de texto requeriría tener un equipo más poderoso de computación. En los resultados que se obtienen se puede ver que aunque el tiempo de procesamiento para encripción del algoritmo de llave pública es mayor al de los algoritmos de llave privada, esto se puede aprovechar para crear archivos más

pequeños y más manejables, y con una seguridad relativamente mayor a los ejemplos dados por programas que manejan algoritmos de llave privada ya que dependen básicamente de que no se descubra una sola llave privada, en cambio el algoritmo de llave pública presenta dos llaves públicas y una llave privada, todas estas se generan a partir de tres números que pueden tener una longitud de hasta 200 dígitos, y al agregar unas cuantas operaciones y mayor reconocimiento de caracteres se hace mas difícil el éxito de los ataques de criptoanálisis. El efectuar un ataque sobre un párrafo codificado de esta manera sería un tanto difícil, ya que si se hiciera sobre un párrafo codificado con el algoritmo RSA con un módulo de 129 hoy en día se terminaría a cabo en unos cuantos meses o semanas, con las operaciones que se agregaron aumentaría el tiempo necesario para que el criptoanálisis tenga éxito. De igual forma se trabajo en el algoritmo de llave privada implementado en MAPLE, en agregándole algunas operaciones, pero sin afectar su estructura básica DES.

Como una posible línea para futuras investigaciones respecto al tema de la seguridad y criptografía, se propone un estudio más profundo para desarrollar nuevos algoritmos de encripción que se encarguen de encriptar de manera efectiva, rápida y que permita también el transporte de la información, sin que esto signifique un decaimiento en el desempeño del sistema. Lo ideal sería que el nuevo algoritmo se adapte a los protocolos de transferencia de archivos, correos, mensajes instantáneos, transferencias entre teléfonos celulares, redes inalámbricas, y en general, a todo dispositivo, tecnología y protocolo que transporte información de un lado a otro. Una más de sus características sería que se puedan agregar mejoras para que el algoritmo resista una posible perdida de paquetes de información, esto se puede presentar en la transferencia de los archivos. Normalmente se necesitan todos los bloques de información para poder reconstruir un mensaje codificado. Algunos de los algoritmos de encripción diseñados posteriormente al RSA y DES son seguros, pero el número de operaciones que presentan hacen que se necesiten muchos recursos. Aquí se debe buscar que el algoritmo presente una seguridad similar a la de los sistemas de llave pública, para comprobar ello se pueden emular ataques informaticos sobre los algoritmos de encripción. Si se logra obtener un algoritmo de encripción que tenga una perfecta funcionalidad con los protocolos usados para las transferencias entre dispositivos, los más beneficiados, serían la comunidad informática y la seguridad.

REFERENCIAS BIBLIOGRAFICAS

[1] IP Security: Building Block for the Trusted Virtual Network
Intel Corporation Whitepaper, 2000
http://www.intel.com./network

[2] Cryptography and network security: Principles and practice
William Stallings, 1998, 2nd Edition
Prentice Hall

[3] Computer security problems growing
Paul Festa, CNET News.com
March 5, 1998.

[4] "Smurf" attack hits Minnesota
Paul Festa, CNET News.com
March 17, 1998.

[5] Hackers Shut FBI Site
Kathleen Ohlson, Computerworld Online, May 28, 1999
http://www.pcworld.com/news/article/0,aid,11177,00.asp

[7] FBI, Industry Scramble to Stop Hack Attacks
Cameron Crouch and Tom Mainelli, PC World, February 09, 2000
http://www.pcworld.com/news/article/0,aid,15202,00.asp

[8] Hackers Hammer the Web
Martyn Williams, IDG News Service, February 09, 2000
http://www.pcworld.com/news/article/0,aid,15186,00.asp

[10] Network Researchers Track the Worldwide Spread of the "Code Red" Worm
Volume 5, Issue 15, July 25, 2001
http://www.npaci.edu/online/v5.15/codered.html

[11] Computer attacks rising, security firm reports
Reuters
http://www.siliconvalley.com/mld/siliconvalley/5098623.htm

[12] Security attacks jump 80 percent
Robert Lemos, CNET News.com, 4th April 2003
http://news.zdnet.co.uk/story/0,t281-s2132972,00.html

[13] RIAA Site Under Attack--Again
Scarlet Pruitt and Ashlee Vance, IDG News Service, February 07, 2003
http://www.pcworld.com/news/article/0,aid,109269,00.asp

[14] Army Server Hacked
Paul Roberts, IDG News Service
Tuesday, March 18, 2003

[15] Al-Jazeera Sites Hit With Denial-of-Service Attacks
Paul Roberts, IDG News Service, March 26, 2003
http://www.pcworld.com/news/article/0,aid,110005,00.asp

[16] Security in open systems
Nikos Drakos, Computer Based Learning Unit, University of Leeds, Copyright © 1993, 1994
http://csrc.nist.gov/publications/nistpubs/800-7/node2.html

[17] The Internet. A global Telecommunications Solution.
Lauren Mathy, Christopher Edwards and David Hutchinson from Lancaster University.
IEEE Network, Volume: 14 Issue: 4 , Jul/Aug 2000
Page(s): 46 -57

[18] Security Protocols in the Internet New Framework.
Sierra, J.M.; Ribagorda, A.; Muñoz, A.; Jayaram, N.
Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on, 1999
Page(s): 311 –317

[19] The Internet Protocol Version 6.
Lee, D.C.; Lough, D.L.; Midkiff, S.F.; Davis, N.J., IV; Benchoff, P.E.
IEEE Network, Volume: 12 Issue: 1, Jan.-Feb. 1998
Page(s): 28 –33

[20] Is IPv6 Finally Gaining Ground?
Lawton, G.,*Computer,* Volume: 34 Issue: 8, Aug. 2001
Page(s): 11 –15

[21] IPv6 – Future Approval Networking.
Hui Huang; Jian Ma
Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on, Volume: 2, 2000
Page(s): 1734 -1739 vol.2

[22] New Possibilities Offered by IPv6
Loukola, M. V. And Skytta, J.O.
Computer Communications and Networks, 1998. Proceedings. 7th International Conference on
Page(s): 548 –552

[23] Deploying IPv6
Durand, A., IEEE Internet Computing , Volume: 5 Issue: 1, Jan.-Feb. 2001
Page(s): 79 –81

[24] The never-ending saga of Internet security: why? how? and what to do next?
Rabinovitch, E.
IEEE Communications Magazine , Volume: 39 Issue: 5 , May 2001
Page(s): 56 –58

[25] Seguridad Informatica. Sus implicancias e implementación
A.S.S. Borghello, Cristian Fabian, Tesis Licenciatura en Sistemas, Universidad Tecnológica Nacional. Septiembre de 2001

[26] The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus
Version 3.23 May 29, 2003, Copyright © 2001-2003, The SANS Institute
http://www.sans.org/top20/

[27] Introducción a UNIX
Azfal Amir, Prentice Hall Iberia,
Madrid , 1997

[28] Solaris™ Operating Environment Security
Alex Noordergraaf and Keith Watson, Suns Blueprints™ On-line, December 2002
http://www.suns.com/blueprints

[29] Packets found on an Internet
Bellovin, S., Computer Communications Review
July 1993.

FUENTES CONSULTADAS

[29] Implementing IPv6.
Mark A. Miller, M&T Books.
Second Edition. 2000

[30] Security at the Internet layer
Oppliger, R., Computer, Volume: 31 Issue: 9 , Sept. 1998
Page(s): 43 –47

[31] Future trends in Internet security
Al-Salqan, Y.Y., Distributed Computing Systems, 1997, Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of
Page(s): 216 –217

[32] Security in Computing
Charles P. Pfleeger, 2nd Edition, 1997
Prentice Hall

[33] Network firewalls
Bellovin, S. And Cheswick W., IEEE Communications Magazine, Volume: 32 Issue: 9 , Sep 1994
Page(s): 50 -57

[34] Limitations of the kerberos authentication system
Bellovin, S. and Merrit, M.
Computer Communications Review
October 1990

[35] Principles of key management
Fumy, S., and Landrock P.,IEEE Journal on selected Areas in Communications
Volume: 11 Issue: 5 , Jun 1993
Page(s): 785 -793

[36] The Story of Non-Secret Encryption
Ellis, J., CESG Report, 1987
http://www.cesg.gov.uk/ellisint.htm